

Intego VirusBarrier X5

Manuel de l’utilisateur



Intego VirusBarrier X5 pour Macintosh

Intego
www.intego.com

Sommaire

1- A propos d’Intego VirusBarrier X5

Présentation d’Intego VirusBarrier X5

Intego VirusBarrier X5 est la solution de sécurité antivirus simple, rapide et non intrusive pour les ordinateurs Macintosh. Ce programme offre une protection efficace contre les virus et les maliciels de tous types, venant de fichiers ou d’applications infectés résidant sur CD, DVD ou d'autres supports amovibles, ou contenus dans des fichiers téléchargés sur Internet ou sur d’autres types de réseaux.

VirusBarrier X5 protège votre Mac contre les virus en examinant constamment tous les fichiers lus et écrits par votre ordinateur, ainsi qu'en surveillant toute activité suspecte qui peut être le signe d'un virus agissant sur des applications ou d'autres fichiers. Grâce à VirusBarrier X5, vous pouvez être certain que votre Macintosh dispose de la meilleure protection possible contre les virus de tous types.

VirusBarrier X5 fonctionne en tâche de fond et inspecte toutes les opérations effectuées par votre Mac en vue de détecter des virus. Il connaît les signatures uniques de tous les virus Macintosh identifiés et, dès qu’un nouveau virus est découvert, le Centre de recherche de virus d’Intego s’active pour fournir des définitions de virus mises à jour, téléchargeables à l’aide d'Intego NetUpdate.

Vous avez accès aux mises à jour des définitions de virus pendant un an à compter de la date d'installation de VirusBarrier X5. Après cette période, des abonnements additionnels, permettant de conserver l’accès aux mises à jour des définitions de virus, sont disponibles auprès d’Intego ; vous pouvez vous abonner via NetUpdate.

VirusBarrier X5 repose sur des concepts très spécifiques. L’idée clé est la suivante : une fois installé et configuré, un programme antivirus ne doit pas nécessiter l’intervention de l’utilisateur tant qu’un virus n’a pas été détecté. La philosophie de VirusBarrier X peut se résumer en trois qualificatifs : simple, rapide et non intrusif.

Simple

VirusBarrier X5 est le programme antivirus le plus facile à utiliser. Une fois installé, il fonctionne en tâche de fond, veillant minutieusement sur votre Mac, et il vérifie vos fichiers en toute discrétion.

Rapide

VirusBarrier X5 est rapide et efficace. Il ne ralentit pas votre Mac et vous pouvez travailler normalement pendant qu'il est actif. À chaque création, ouverture, fermeture ou enregistrement de fichier, VirusBarrier X5 vérifie que le fichier est sain.

Non intrusif

VirusBarrier X5 est non intrusif. Il ne vous assaille pas de questions suspicieuses chaque fois que vous installez un programme, pas plus qu'il ne vous importune en générant sans cesse des fausses alertes. Une fois le logiciel installé, vous n'en remarquerez pas la présence, jusqu'à ce qu'il détecte un virus et génère une alerte. Par ailleurs, vous n'avez pas besoin de désactiver VirusBarrier X5 lors de l'installation d'un nouveau logiciel, quelles que soient les préconisations du programme d'installation ou du manuel de ce dernier. VirusBarrier X5 peut fonctionner en permanence, en tâche de fond, protégeant ainsi votre Mac sans nul besoin de s'en soucier.

VirusBarrier X5 est compatible avec le système d'exploitation Mac OS X 10.4 ou ultérieur (Tiger et Leopard).

Fonctionnalités de VirusBarrier X5

Analyse de virus

VirusBarrier X5 fonctionne de plusieurs façons. Tandis que son scanner temps réel est constamment en veille, afin de protéger votre Mac contre les assauts éventuels de virus et de maliciels, il peut fonctionner en mode manuel. Vous pouvez ainsi lui demander d’analyser un disque ou un volume partagé de votre réseau et des iPhones ou des iPod touch connectés à un Mac.

Réparations automatiques

Quand VirusBarrier X5 lance son scanner temps réel, il peut réparer les fichiers infectés qu’il détecte en éliminant les virus, si possible. Dans ce mode, vous n’avez pas besoin de vous soucier de l’activité de VirusBarrier X5 – vous savez simplement qu’il est là, prêt à intervenir au cas où un virus ou un fichier suspect serait détecté.

Zone de quarantaine

Si vous ne voulez pas réparer les fichiers automatiquement, vous pouvez régler VirusBarrier X5 pour qu'il mette les fichiers dans une zone spéciale de quarantaine. Quand les fichiers sont mis en quarantaine, ils ne peuvent être ni ouverts ni lus, ce qui assure qu'ils ne puissent pas infecter votre Mac. Cette fonction est utile aux administrateurs qui veulent vérifier les fichiers avant de lancer les fonctions de réparation de VirusBarrier X5.

Scanner manuel

Vous pouvez utiliser VirusBarrier X5 pour analyser manuellement vos fichiers, disques ou volumes, et vous assurer qu’ils sont exempts de virus. Il est recommandé d’effectuer cette opération dès la première installation du programme, afin de vous assurer que votre Mac est sain. Vous pouvez analyser les fichiers individuels par glisser-déposer sur l’icône du programme ou sur son Orbe quand il fonctionne au premier plan. Nous recommandons également de scanner votre Mac manuellement à chaque installation de nouvelles mises à jour des définitions de virus ; une option permet de lancer automatiquement le scanner après chaque mise à jour.

Mode turbo

VirusBarrier X5 propose un Mode turbo qui accélère les analyses. Lors de l'analyse de votre Mac, VirusBarrier X5 enregistre des informations sur tous les fichiers examinés. Tant que ces fichiers ne sont pas mis à jour, VirusBarrier X5 ne les rescanne pas, ce qui accélère le processus.

Historique d'analyse

VirusBarrier X5 affiche un rapport complet sur toute son activité, et particulièrement sur les virus ou les fichiers douteux trouvés. Vous pouvez consulter cet historique pour connaître les fichiers corrompus ou les applications infectées, les virus qui les ont contaminés et s'ils ont été réparés. Grâce à l'export automatique des historiques, vous pouvez faire tourner les fichiers d'historique et les sauvegarder par ordre chronologique.

Icône, Dock et menu contextuel

Vous pouvez analyser les fichiers, dossiers ou volumes en les faisant glisser sur l'icône VirusBarrier X5 dans le Dock. Le menu contextuel sert à analyser rapidement des éléments depuis le Finder.

Alertes de virus

VirusBarrier X5 dispose d'options d'alerte pour que vous soyez averti en cas de détection d'un virus, lors de son utilisation en tâche de fond. Plusieurs types d'alerte sont disponibles : écran d'alerte, message vocal ou envoi de message électronique à une adresse déterminée. Cette solution peut s'avérer utile si vous souhaitez utiliser VirusBarrier X5 sur des ordinateurs connectés à un réseau et avertir un administrateur réseau ou le propriétaire de l'ordinateur, lorsque ceux-ci sont éloignés de leur poste.

NetUpdate

VirusBarrier dispose du programme Intego NetUpdate pour vérifier automatiquement l'existence de mises à jour du programme ou de nouvelles définitions de virus. Vous réglez NetUpdate, pour que la vérification des mises à jour respecte une fréquence quotidienne ou hebdomadaire. Vous pouvez vérifier à tout moment le statut des mises à jour, grâce au widget NetUpdate inclus avec VirusBarrier X5.

Présentation du manuel d’utilisation

Ce manuel d’utilisation contient des informations détaillées sur l’installation, l’utilisation et la mise à jour de VirusBarrier X5, ainsi qu’un glossaire sur la terminologie des virus.

Nous vous invitons à lire l’introduction aux modes de fonctionnement des virus (chapitre 2), puis à consulter la procédure de prise en main rapide (chapitre 3). Nous recommandons la description des fonctionnalités de VirusBarrier X5 et du mode d'analyse de votre Mac (chapitres 4 et 5), et des réglages et préférences (chapitre 6). Pour des informations détaillées sur les virus, consultez le glossaire (chapitre 9).

2 - Introduction aux virus informatiques

De multiples raisons de se protéger

Votre Mac contient des informations et des fichiers importants. Si vous l'utilisez dans un cadre professionnel, vous devez avoir une idée du coût que la perte de ces fichiers entraînerait, aussi bien en temps qu'en argent. En tant qu'utilisateur particulier, vous avez certainement des fichiers que vous n'aimeriez pas perdre. En tous cas, si un virus devait effacer tous vos fichiers, quelle que soit leur importance, la réinstallation du système et de tous vos programmes vous prendrait beaucoup de temps.

La menace des virus est réelle. Le nombre de virus découverts quotidiennement ne cesse d'augmenter. Bien que les ordinateurs Macintosh soient relativement privilégiés par rapport aux systèmes sous Windows, il existe toujours un risque de voir des virus existants ou nouveaux s'infiltrer dans votre Mac et corrompre vos fichiers.

Virus informatiques

Rien ne peut plus effrayer un utilisateur que d'insinuer que son ordinateur est peut-être atteint d'un virus. En fait, les utilisateurs ont tous entendu parler des dégâts que pouvaient causer les virus. Si ces histoires peuvent en faire sourire certains, en revanche personne ne peut rester indifférent en découvrant que son ordinateur est infecté par un virus.

Le risque lié aux virus est très répandu, et il est aggravé par l'échange quotidien et continu des fichiers. Un virus peut se propager aussi rapidement qu'une épidémie de grippe, même à partir d'un seul ordinateur. Qu'est-ce au juste qu'un virus informatique ? Comment fonctionne-il ? Pourquoi est-il si dangereux ?

C'est au début des année 1980, lors de la mise en circulation d'un programme informatique autoreproducteur, que le terme virus fut appliqué pour la première fois aux ordinateurs.

Un virus n'est rien d'autre qu'une séquence de code exécutable attachée à un fichier ou une application. Les virus ne s'attrapent pas dans l'air – il leur faut un moyen de transmission, tel qu'un CD, un DVD, ou un fichier envoyé en pièce jointe à un message ou téléchargé via Internet. À l'instar des virus qui envahissent notre organisme, les virus informatiques tentent de se reproduire après avoir infecté un hôte et s'attachent à d'autres fichiers et applications. Ils se reproduisent, attaquent de nouveaux hôtes, et le processus est sans fin.

Les virus sont de petits programmes informatiques – plus ils sont petits, plus ils sont redoutables, car ils se dissimulent plus facilement dans les fichiers et applications et échappent ainsi à la détection. Ils sont écrits dans un seul but : se reproduire et se propager aux autres ordinateurs. Bien que certains virus soient inoffensifs ou ne provoquent que l'apparition d'un message à l'écran, la plupart d'entre eux produisent des effets néfastes sur les ordinateurs et les fichiers. Bien qu'il existe des exemples notables de virus écrits sans aucune intention de nuire, le plus souvent, leurs auteurs cherchent à détruire des fichiers et transmettre ces virus à d'autres ordinateurs. Les virus sont très souvent écrits pour entraîner des dégâts économiques, soit par l'envoi des données personnelles à des ordinateurs malveillants, soit par le détournement de l'activité web d'un utilisateur. Les virus, autrefois écrits par des adolescents en crise et des pirates surdoués, sont maintenant créés par des criminels aux objectifs très clairs.

De l'ordinateur personnel à l'ordinateur de réseau d'entreprise, un virus informatique peut contaminer n'importe quelle machine, du moins si aucune précaution n'a été prise. La meilleure précaution passe par l'utilisation de VirusBarrier X5 et, surtout, la tenue à jour du programme et des définitions de virus.

Mode de fonctionnement des virus informatiques

Dans l'esprit de la plupart des utilisateurs, le terme "virus informatique" englobe de nombreux types de "maliciels", dont certains ne sont pas des virus : par exemple, les chevaux de Troie et les vers fonctionnent de manière différente et ne se reproduisent pas systématiquement comme le font les virus. Pourtant, on a souvent tendance à les associer à la famille des virus. Bien que ces programmes soient malveillants et puissent gravement endommager votre ordinateur et vos fichiers, ils fonctionnent différemment.

Un vrai virus est une courte séquence de code informatique – autrement dit, des instructions de programmation – qui peut être exécutée ou mise en œuvre sur le type d'ordinateur visé. Ainsi, les virus conçus pour s'attaquer aux ordinateurs fonctionnant sous Windows n'ont aucun effet sur les ordinateurs Macintosh, et vice versa. Cela dit, si vous utilisez Windows sur un Macintosh basé sur Intel, vous devez également vous pencher sur la protection de ce système d'exploitation. La gamme Dual Protection d'Intego protège votre Mac ainsi que votre installation Windows.

Une fois activés sur l’ordinateur, les virus effectuent deux opérations. Ils essaient d’abord d’exécuter leur code afin de mener à bien leur mission destructrice, puis ils tentent de se reproduire en copiant ce code dans d’autres fichiers, applications, disques ou volumes réseau. Voici un exemple des dégâts que pourrait causer un virus fictif sur votre Macintosh. (Le cas présente les effets d’un cheval de Troie, qui sont faciles à comprendre.)

> Un ami ou un collègue vous a envoyé un programme infecté via Internet. Bien que l’on vous ait conseillé de ne pas ouvrir de pièces jointes en provenance d’inconnus, vous décidez d’ouvrir le fichier puisque vous estimez qu’il provient d’une source sûre. Supposons qu’il s’agisse d’une application ; par exemple, une de ces cartes de vœux animées qui circulent beaucoup. Vous double-cliquez sur le fichier, ce qui lance l'application. Cependant, au cours de son exécution, elle active sa signature virale et copie un code parasite dans votre système. En même temps, elle se répand sur le réseau local de votre entreprise, en se copiant sur d'autres fichiers. Une fois la présentation terminée, vous quittez l’application. Vous n’avez encore rien remarqué d’anormal sur votre ordinateur, car le code a été défini de manière à ne produire ses effets qu’au redémarrage de l’ordinateur.
>
> Le lendemain matin, vous arrivez au travail et vous démarrez votre ordinateur, mais vous remarquez qu’il est plus long à démarrer que d’habitude. Lorsqu’il a enfin démarré, vous trouvez qu’il fonctionne très lentement. Vous allez pour ouvrir le rapport urgent à terminer avant le déjeuner et constatez que le fichier a disparu. Vous parcourez le disque dur et découvrez avec effroi que des dizaines, voire des centaines de fichiers ont disparu. C’est alors que vous réalisez que, la veille, vous avez oublié de sauvegarder votre disque dur et que vous n’avez aucune copie récente de ces fichiers.
>
> Vous avez déjà envoyé cette carte de vœux animée à d’autres amis, mais vous n’avez pas établi de lien entre la carte et la disparition de vos fichiers. Ce n’est que quelques heures plus tard, quand l’un de vos amis vous apprend que la carte de vœux animée a affecté son ordinateur, que vous prenez conscience de ce qui s’est passé.

Comme le montre cet exemple, une simple infection de virus peut avoir des conséquences graves, et non seulement pour vous, mais aussi pour vos correspondants. Un des plus gros problèmes liés aux virus est actuellement l’échange continu de fichiers via Internet, et les

ordinateurs peuvent être infectés très rapidement. En vous protégeant avec Intego VirusBarrier X5, vous protégez aussi les autres.

Différents types de virus

On peut diviser les virus en deux types différents, selon les éléments de l'ordinateur auxquels ils s'attaquent. Les virus du premier type sont appelés virus système, car ils s'attaquent aux fichiers système. Les virus du deuxième type, appelés virus de fichiers, infectent les applications et les fichiers de données.

Virus

Un virus informatique est un petit programme qui agit comme un parasite. Vivant dans un fichier hôte ou un programme, il est capable d'infecter les fichiers et les applications, de se reproduire et de se propager à d'autres ordinateurs par le biais des fichiers et des applications infectés. Il n'est guère surprenant que l'on utilise des termes habituellement appliqués aux maladies pour parler des virus informatiques : ils agissent d'une manière très comparable.

Les virus qui s'attaquent au système sont parmi les plus destructeurs. Les dégâts qu'ils peuvent causer sont tels que la réinstallation complète du système et même le reformatage du disque dur peuvent s'avérer nécessaires, tout comme la vérification de toutes les sauvegardes pour s'assurer qu'elles sont saines.

Les virus de fichiers diffèrent des virus système car ils s'attachent aux fichiers de données, plutôt qu'aux applications, et leurs hôtes ont besoin de programmes spécifiques pour produire leurs effets destructeurs. Ces virus viennent souvent dans des pièces jointes aux messages électroniques, qui activent leur code nuisible une fois ouvertes.

Certains virus agissent très rapidement, d'autres sont programmés pour se manifester à un moment déterminé. Certains se contentent uniquement de se propager à d'autres disques et volumes, mais tous les virus système présentent un danger potentiel, comme celui de supprimer tous vos fichiers.

Chevaux de Troie

Le nom "Cheval de Troie" est tiré d'un épisode de la guerre qui opposa les Grecs et la cité de Troie il y a plus de deux mille ans. Les Grecs édifièrent un cheval en bois gigantesque et creux et l'offrirent soi-disant en cadeau aux Troyens en vue de terminer la guerre. Bien que ce geste laissât certains Troyens perplexes, le cheval fut amené à l'intérieur de leur forteresse. La même

nuit, les guerriers grecs sortirent du cheval, ouvrirent les portes de la cité et les troupes grecques stationnées à l'extérieur la prirent d'assaut.

Bien sûr, personne n'a jamais conseillé aux Troyens de ne pas ouvrir les pièces jointes. Les chevaux de Troie dont on se préoccupe aujourd'hui sont des programmes apparemment inoffensifs, prétendant exécuter certaines tâches mais contenant en fait un code parasite ou des virus. Dans de nombreux cas, les chevaux de Troie sont potentiellement plus dangereux que les autres virus. C'est l'exemple du cheval de Troie RSPlug (ou DNSChanger), que le Centre de recherche de virus d'Intego a découvert en 2007. Ce maliciel, déguisé en codec vidéo (logiciel pour visionner des vidéos sur un site web), a modifié le serveur DNS sur un Mac pour détourner son trafic web.

Vers

Les vers constituent la forme la plus ancienne des programmes informatiques parasites. Pour se propager, ils ne s'attachent pas à des fichiers et des applications, et leur identification peut être très difficile. Ils se propagent sur des réseaux et, dès qu'ils ont trouvé de nouveaux hôtes, ils peuvent réaliser leurs actions nuisibles.

Virus macro

De nombreux programmes offrent la possibilité de créer des macro-commandes. Ces petits programmes utilisent les fonctions internes d'une application pour "enregistrer" et "exécuter" des séquences de commandes courantes. D'autres applications offrent un langage macro plus puissant combinant des commandes de menus et un langage de programmation. Les fonctions macro de programmes comme Microsoft Word et Excel, pour les versions antérieures à Office 2008, sont basées sur le langage Visual Basic de Microsoft, qui s'apparente au langage de programmation Basic. Plusieurs milliers de virus macro ont été découverts, et la plupart concernent Microsoft Word et Excel.

Le vrai danger des virus macro vient du fait qu'il s'agit de virus multi-plates-formes. Un virus macro qui peut attaquer Microsoft Word pour Windows peut également endommager Word sur un Mac. Si les auteurs de virus macro prennent souvent pour cible les programmes Microsoft, c'est en partie parce que ces applications permettent l'ajout de macros dans les fichiers de données. Par le passé, on craignait uniquement les virus transmis par les applications, car un virus doit s'exécuter avant d'agir et seules les applications le permettaient. Mais l'approche de Microsoft Visual Basic est différente – si vous souhaitez utiliser une macro, vous pouvez soit

l’exécuter à partir de votre modèle, soit l’ajouter à un fichier de données. Au début, les utilisateurs furent surpris, car ils pensaient que rien ne "s’exécutait" à l’ouverture d’un fichier de traitement de texte ou de tableur. Mais ces fichiers peuvent en fait contenir des "programmes" et accomplir des choses totalement inattendues.

Si le langage macro offre la possibilité de modifier les fichiers, un virus macro pourra se copier lui-même dans d’autres fichiers utilisés par la même application. Le virus peut alors se propager lors de l’ouverture d’autres fichiers, de la création de nouveaux fichiers, ou du transfert de fichiers à un autre utilisateur.

Les virus macro sont polyvalents : certains vont seulement altérer l'environnement de leur programme, par exemple, modifier ou supprimer des menus ou des commandes. D'autres peuvent corrompre ou supprimer des fichiers, masquer certaines fonctions d’applications, et plus encore. Pour couronner le tout, ce sont des virus multi-plates-formes qui endommagent les Macintosh, les PC fonctionnant sous Windows, ainsi que Windows fonctionnant sur un Mac.

Il faut noter que les langages macro sont des outils très puissants et potentiellement très utiles. Toutes les macros ne sont pas des virus. La fonction de Microsoft Word et Excel alertant de la présence d’une macro dans les documents n’incite guère à utiliser la fonction macro. Le vrai problème vient du fait que les macros sont stockées dans des fichiers de données, plutôt que dans des fichiers séparés. Les utilisateurs pourraient échanger des macros stockées en fichiers séparés, avec l’assurance que les fichiers ouverts ne contiennent que des données. Malheureusement, ce principe de stockage en fichier de données entraîne trop de méfiance face aux macros, au lieu d'inciter à tirer profit de leurs propriétés pour améliorer des fonctions.

VirusBarrier X5 détecte tous les virus macro connus de Microsoft Word et Excel ; il est mis à jour dès la découverte de nouveaux virus macro.

Modes de propagation des virus

Les virus peuvent se propager via des fichiers infectés contenus sur des CD, des DVD et d'autres supports amovibles, ou téléchargés sur Internet. Ils peuvent être envoyés en pièces jointes par courrier électronique. Les fichiers infectés ne peuvent pas libérer leurs virus tant qu’ils n’ont pas été ouverts ou lus. Vous ne risquez donc pas de propager un virus par simple copie d’une application ; seule l’exécution de l’application vous expose à ce risque.

VirusBarrier X5 protège votre ordinateur contre ces virus en analysant les fichiers à l'ouverture, l'écriture ou l'utilisation. Dès que vous manipulez un fichier, celui-ci est aussitôt analysé. Si VirusBarrier X5 détecte un virus, le fichier ou l'application est désinfecté ou rendu inexploitable.

Modes de protection possibles contre les virus

Pour vous prémunir contre les virus informatiques, il suffit d'appliquer quelques règles simples. La première, et certainement la plus importante, est d'utiliser VirusBarrier X5. Votre ordinateur est alors constamment surveillé et les virus sont recherchés automatiquement. VirusBarrier X5 constitue la meilleure protection pour votre Macintosh ; il œuvre en tâche de fond pour assurer la sécurité de votre ordinateur.

Pour rester protégé contre les nouveaux virus, vous devez mettre à jour VirusBarrier X5 de façon régulière. Intego NetUpdate simplifie cette opération, et peut même l'automatiser. Il est conseillé de vérifier les mises à jour au moins une fois par semaine. En cas de découverte de nouveaux virus importants, Intego affiche, aussi rapidement que possible, des informations sur le site web (www.intego.com), ainsi que sur le Mac Security Blog d'Intego, disponible en anglais (http://blog.intego.com). Le Centre de recherche de virus d'Intego fonctionne en continu et réagit aux premiers signes d'apparition de nouveaux virus.

Si vous pensez avoir contracté un nouveau virus, reportez-vous au chapitre 7, **Support technique**, pour savoir comment contacter Intego.

Pour vous protéger utilement, il est conseillé d'utiliser uniquement des logiciels provenant de sources sûres. Les logiciels piratés peuvent contenir des virus ou même un cheval de Troie inattendu. Veillez à n'installer que les logiciels dont vous connaissez la provenance.

Par ailleurs, vous devez faire preuve de la plus grande vigilance en ce qui concerne les fichiers reçus par courrier électronique ou via Internet. On a vu, par l'exemple du cheval de Troie, combien l'ouverture candide d'une pièce jointe pouvait être périlleuse. On a l'habitude de dire qu'il ne faut jamais ouvrir de pièces jointes provenant d'inconnus. Or, de nombreux virus se sont propagés par l'envoi de pièces jointes entre amis et collègues de travail. VirusBarrier X5 vous protège en analysant chaque fichier ouvert et en éliminant automatiquement tous les virus connus. Si vous travaillez sur un ordinateur en réseau et VirusBarrier X5 détecte un virus dans

une pièce jointe, veillez à contacter immédiatement votre administrateur réseau afin qu'il supprime le fichier infecté du serveur de messagerie de l'entreprise.

Bien que VirusBarrier X5 offre un niveau élevé de protection antivirale, la protection de vos données exige que vous appliquiez une autre règle : sauvegarder régulièrement vos fichiers. Vous devez non seulement sauvegarder les fichiers importants tous les jours, mais également en faire plusieurs sauvegardes. En effet, le support de sauvegarde peut s'endommager ou s'altérer et les sauvegardes ne seraient plus d'aucun secours. Intego Personal Backup X5 offre une solution complète de sauvegarde, le logiciel sait effectuer des sauvegardes automatiques, vous êtes assuré de toujours disposer d'une copie saine de vos données, au cas où un virus viendrait à infecter votre Mac.

Nous vous conseillons une bonne méthode de travail : veiller à faire deux sauvegardes différentes de vos données. C'est une simple assurance. Non seulement vous serez assuré d'avoir des copies saines de vos fichiers dans le cas où vous trouveriez un virus sur votre ordinateur, mais vos données seront à l'abri d'autres types de problèmes, tels que des blocages de disque dur, etc. Vu le coût relativement modique des supports amovibles ou même des CD, des DVD ou des disques durs externes, vous pouvez également sauvegarder votre Système et vos applications. Soyez vigilant ; si, pour quelque raison que ce soit, l'ordinateur se corrompt, la réinstallation du système et des applications vous prendra beaucoup de temps. Si, en revanche, vous avez sauvegardé votre Mac en intégralité, cette opération ne prendra que quelques minutes. Personal Backup X5 dispose d'une gamme complète de fonctionnalités de sauvegarde, y compris les sauvegardes incrémentales, les sauvegardes démarrables de votre système et les synchronisations. En établissant une politique de sauvegarde cohérente, vous pouvez vous assurer qu'en cas de problèmes, vous pourrez reprendre rapidement le travail.

En cas de crainte d’un virus

Quelques symptômes d’infection

Bien que ces symptômes ne signifient pas forcément que votre ordinateur ait subi l’attaque d’un virus, ils peuvent en être le signe :

- Vous constatez des messages d’erreur inattendus,
- Votre Macintosh se bloque de façon inexplicable,
- Les applications quittent de manière inattendue,
- Votre système a l'air plus lent que d’habitude,
- Vous découvrez de nouveaux comptes utilisateur que vous n'avez pas créés,
- L’espace disque semble avoir diminué de manière significative bien que vous n’ayez pas ajouté de nombreux fichiers.

Si votre Mac commence à présenter l’un de ces symptômes, plusieurs moyens permettent de vérifier si le problème vient d’un virus ou d'un logiciel.

Nous vous conseillons d'abord de lancer Intego NetUpdate et de vérifier que vous disposez bien des dernières définitions de virus pour VirusBarrier X5. Vous pouvez ensuite scanner votre Mac pour vous assurer qu'il est exempt de maliciel.

Puis, si le problème n'est toujours pas résolu, il est probable qu'il s'agisse d'un disque corrompu. Vous pouvez exécuter le programme Utilitaire de Disque d’Apple. Ce programme a été conçu pour diagnostiquer les problèmes de disque dur et en résoudre la plupart. Il est installé par défaut dans le dossier Utilitaires de votre dossier Applications. Si le programme Utilitaire de Disque identifie des problèmes qu’il ne peut résoudre, vous devrez vous procurer un logiciel commercial de maintenance de disque.

Si le problème persiste, il se peut qu’un logiciel récemment installé soit à l’origine du problème. En effet, la plupart des problèmes informatiques sont dus à des conflits de logiciels. Si vous venez d’installer de nouveaux logiciels, essayez de les désinstaller et vérifiez si le problème persiste.

Votre problème peut être causé par un périphérique, tel qu'un lecteur externe, un périphérique USB connecté à votre ordinateur, le pilote de votre imprimante, etc. À nouveau, vérifiez si le problème persiste lorsque ces périphériques et leurs pilotes sont désactivés.

Pour de plus amples informations, consultez la section Support du site web d'Apple (www.apple.fr). Vous y trouverez peut-être une solution.

Enfin, si vous pensez être en possession d'un fichier infecté, vous pouvez envoyer une copie de ce fichier au Centre de recherche de virus d'Intego. Pour d'informations, reportez-vous au chapitre 7, **Support technique**.

Mesures de précaution élémentaires

VirusBarrier X5 veille dorénavant sur votre Macintosh ; cependant, vous devez vous habituer à respecter quelques principes de base pour assurer la protection permanente de vos fichiers.

- Sauvegardez régulièrement vos fichiers. Avec Intego Personal Backup X5, réalisez des sauvegardes automatiques de vos fichiers utilisateur et créez des sauvegardes démarrables de tout votre Mac.
- Créez plusieurs copies de vos fichiers les plus importants.
- Quand vos supports amovibles "voyagent" vers d'autres ordinateurs ou si vous les confiez à d'autres utilisateurs, veillez à les protéger en écriture en faisant coulisser la languette de protection (si possible). Utilisez VirusBarrier X5 pour analyser les disques durs externes, les clés USB ou les cartes de mémoire flash que d'autres vous prêtent pour transférer des fichiers.
- Sauf nécessité absolue, ne désactivez pas VirusBarrier X5 : vous n'avez pas besoin de le désactiver pour installer de nouvelles applications, même si certains programmes d'installation le demandent.
- N'utilisez pas de logiciels piratés : non seulement vous enfreignez les lois, mais ces logiciels risquent d'être porteurs de virus.
- De même, n'installez les programmes que si vous êtes certain de l'intégrité de leur emballage d'origine.
- Pensez à utiliser régulièrement NetUpdate pour vérifier que vous avez bien la dernière version à jour de VirusBarrier X5.

Pour éviter toute incompatibilité, utilisez uniquement VirusBarrier X5 pour la protection antivirus de votre ordinateur.

Configuration matérielle et logicielle requise

- Tout ordinateur compatible Mac OS X (supporté officiellement par Apple)
- Mac OS X 10.4 ou ultérieur, ou Mac OS X Serveur 10.4 ou ultérieur

Installation de VirusBarrier X5

Pour les informations relatives à l'installation et la sérialisation de VirusBarrier X5, consultez le Manuel de Démarrage Intego, inclus avec votre copie du programme. Si vous avez acheté le logiciel par téléchargement sur le site web d'Intego, ce manuel se trouve dans l'image disque qui contient le logiciel. Si vous avez acheté VirusBarrier X5 sur un CD ou un DVD, ce manuel se trouve sur le disque.

3 - Prise en main rapide

Interface de VirusBarrier X5

Dès que vous avez installé VirusBarrier X5 et redémarré votre Macintosh, il commence automatiquement à surveiller l'ordinateur. VirusBarrier X5 est conçu pour être simple et non intrusif, et il protège totalement votre ordinateur sans que vous ayez à intervenir.

Une fois le programme installé, vous pouvez simplement le laisser fonctionner de manière indépendante. Cependant, nous vous conseillons de régler NetUpdate pour qu'il vérifie automatiquement la présence de mises à jour du programme, ou de le faire manuellement au moins une fois par semaine.

Pour ouvrir VirusBarrier X5, modifier les réglages ou effectuer une analyse manuelle, vous pouvez :

- Double-cliquer sur l'icône VirusBarrier X5 dans le dossier Applications, ou
- Sélectionner le menu Intego > VirusBarrier X5 > Ouvrir VirusBarrier X5...

L'application VirusBarrier X5 contient l'Orbe, le bouton **analyser**, ainsi que plusieurs instruments d'affichage d'informations ou de modification des réglages. Pour accéder aux fonctionnalités, cliquez sur les petits boutons de flèche dans l'interface.



L'Orbe de VirusBarrier X5, le grand disque vert au centre de la fenêtre, présente des informations relatives à l'opération en cours. Autour de l'Orbe, se trouvent six “instruments”, des compteurs et des affichages et, sous l'Orbe, le bouton **analyser**.



Le bouton **analyser** sous l'Orbe de VirusBarrier X5 change et reflète sa fonction, telle que analyser, réparer, pause, stop, etc. Par défaut, c'est le bouton **analyser** : si vous cliquez dessus, VirusBarrier X5 va analyser votre Mac à la recherche de virus et d'autres maliciels. En cas de détection, une fenêtre d'alerte vous demande l'action à réaliser. Cependant, quand vous appuyez sur la touche Option, le bouton **analyser** devient un bouton **réparer**, ce qui signifie que VirusBarrier X5 va automatiquement réparer les fichiers contenant des virus ou des maliciels sans demander votre intervention. En appuyant sur la touche Option (Alt) pendant une analyse, le bouton affiche **pause** ; cliquez sur le bouton pour mettre votre analyse en pause.



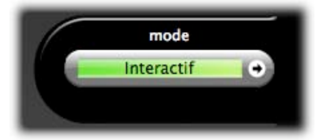
Le bouton **sélectionner** au-dessus du bouton **analyser** permet de sélectionner les volumes, dossiers ou fichiers à analyser à la recherche de virus. Consultez **Sélection des fichiers et lancement du scanner manuel** au chapitre 4, **Analyse de votre Mac avec VirusBarrier X5** pour en savoir plus sur la sélection des éléments à analyser. En appuyant sur la touche Option (Alt), le bouton **sélectionner** devient **naviguer** ; cliquez sur ce bouton pour naviguer dans votre Mac et analyser des fichiers ou des dossiers.

L'instrument **planifications** indique le nombre de planifications prévues et permet de planifier les heures fixes de lancement des planifications. Si des planifications sont en cours, le nombre de planifications actives apparaît entre parenthèses dans l'instrument, suivant le nombre total de planifications prévues. En cliquant sur la flèche, vous pouvez régler des planifications ; consultez **Analyse planifiée** au chapitre 4, **Analyse de votre Mac avec VirusBarrier X5** pour savoir comment planifier.



L'instrument **mode** indique le mode de fonctionnement de VirusBarrier X5. Les divers modes sont les suivants :

- Mode **interactif**, où le programme affiche une alerte, vous demandant que faire quand il découvre des fichiers infectés,
- Mode **réparation**, où le programme répare automatiquement les fichiers infectés, ou
- Mode **quarantaine**, où le programme met les fichiers infectés dans sa zone de quarantaine.



En cliquant sur la flèche, vous pouvez modifier le mode ; consultez **Préférences de scanner** au chapitre 6, **Préférences de VirusBarrier X5** pour savoir comment choisir les modes.

L'instrument **quarantaine** indique le nombre de fichiers présents dans la zone de quarantaine de VirusBarrier X5, et ses compteurs réagissent à l'ajout de nouveaux fichiers. En cliquant sur la flèche, vous allez vers la zone de quarantaine ; consultez **Zone de quarantaine** au chapitre 4, **Analyse de votre Mac avec VirusBarrier X5** pour savoir comment gérer la zone de quarantaine.



Trois instruments offrent des représentations visuelles de la vitesse de VirusBarrier X5 :

L'indicateur d'activité indique l'intensité de travail du ou des processeurs de votre Mac.



L'instrument **mode turbo** indique l'efficacité du mode turbo de VirusBarrier X5. Lors d'une analyse, VirusBarrier X5 mémorise les fichiers qu'il a analysés, et les ajoute à une base de données. Lors de l'analyse suivante de votre Mac, VirusBarrier X5 n'a pas besoin de rescanner tous les fichiers, mais uniquement ceux qui ont été ouverts ou modifiés depuis la dernière analyse. Cependant, quand vous installez des nouvelles définitions de virus, VirusBarrier X5 rescanne *tous* les fichiers, et il remet à zéro la base de données du mode turbo ; cela permet d'assurer que tous les fichiers soient vérifiés par rapport aux nouvelles définitions de virus.

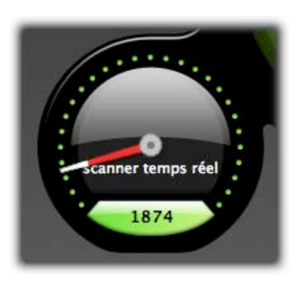
L'instrument **mode turbo** indique, pendant une analyse, le pourcentage de fichiers se trouvant dans la base de données du mode turbo. Quand l'aiguille va vers la zone verte, VirusBarrier X5 gagne du temps en utilisant le mode turbo. Quand elle va vers la zone rouge, VirusBarrier X5 analyse les fichiers pour la première fois, ou analyse ceux qui ont été modifiés depuis la dernière analyse.

Pour réinitialiser la base de données du mode turbo, cliquez sur le bouton de remise à zéro dans cet instrument. Après la remise à zéro, VirusBarrier X5 va commencer du début lors de la prochaine analyse manuelle et vérifier tous vos fichiers.



Note : quand vous utilisez le mode turbo de VirusBarrier X5, le programme écrit des fichiers invisibles, libellés .vbt5, au niveau racine de chaque volume inscriptible qu'il analyse.

L'instrument **scanner temps réel** indique le niveau d'activité du scanner en temps réel de VirusBarrier X5, ainsi que le nombre de fichiers analysés depuis le dernier redémarrage de votre Mac.



Deux autres boutons apparaissent dans la fenêtre.

Le bouton d'historique dans le coin inférieur droit ouvre une liste d'historique, présentant les dates et heures des analyses manuelles et les fichiers infectés ou corrompus détectés.



Le bouton de NetUpdate, étiqueté "Vérifier...", permet de vérifier les mises à jour pour VirusBarrier X5. Le bouton de NetUpdate apparaît dans la barre de statut NetUpdate ; si vous ne voyez pas cette barre, sélectionnez Présentation > Afficher la barre de statut NetUpdate. Pour en savoir plus sur NetUpdate, reportez-vous au Manuel de Démarrage Intego.



Votre priorité : Analyser tout votre disque dur

Les nombreuses fonctionnalités de VirusBarrier X5 protègent votre Mac dès que des virus apparaissent. Avant tout autre opération, nous vous conseillons d'effectuer une analyse complète de votre Mac pour identifier et éliminer tous les virus déjà présents. Voilà la méthode :

Si votre Mac n'a qu'un seul disque dur, ou si vous voulez analyser tous les disques durs connectés à votre Mac, il vous suffit de cliquer sur le bouton **analyser**.

Si vous ne voulez analyser que certains disques durs, procédez comme suit :

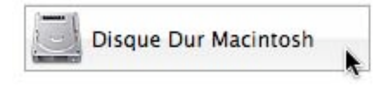
1. Cliquez sur le bouton **sélectionner**.



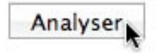
2. Cliquez sur le bouton **Disques durs**.



3. Cliquez sur chaque disque dur à analyser.



4. Cliquez sur le bouton **Analyser**.



Dans les deux cas, VirusBarrier X5 compte d'abord tous les fichiers sur votre Mac, puis il vérifie chaque fichier pour s'assurer qu'il est exempt de virus. Vu que ce processus peut concerner jusqu'à des centaines de milliers de fichiers, il peut durer plusieurs minutes ou même des heures. Vous pouvez toujours utiliser votre Mac pendant que VirusBarrier X5 effectue cette analyse intégrale ; cependant, il est souhaitable d'attendre et de ne pas utiliser votre ordinateur pour d'autres tâches avant de lancer cette vérification initiale ; de même il vaut mieux que l'ordinateur soit branché sur le secteur, au lieu de fonctionner sur batterie.

Pour tous détails sur la procédure au cas où VirusBarrier X5 rencontre un problème, consultez Alertes au chapitre 4, **Analyse de votre Mac avec VirusBarrier X5**.

4 – Analyse de votre Mac par VirusBarrier X5

Analyse de virus

VirusBarrier X5 fonctionne de plusieurs façons. Le scanner en temps réel surveille constamment votre Mac pour la protection contre les virus, et il vérifie automatiquement tous les fichiers lors de leur ouverture et enregistrement. Vous pouvez aussi utiliser le scanner manuel de VirusBarrier X5, pour vérifier, à la demande, tous les éléments (fichiers, dossiers, disques, volumes) sur votre Mac.

Le scanner en temps réel s'assure que votre Mac est constamment protégé en analysant chaque fichier créé, copié, modifié ou enregistré. Cependant, il n'analyse pas les autres fichiers. C'est pourquoi nous suggérons d'effectuer une analyse complète de tous vos fichiers quand vous installez VirusBarrier X5 et après chaque mise à jour des définitions de virus du programme.

Sélection des fichiers et lancement du scanner manuel

Dès son installation, VirusBarrier X5 surveille les fichiers et assure qu'ils sont à l'abri des virus. VirusBarrier X5 vérifie également les fichiers à l'ouverture et à l'enregistrement. Cette fonctionnalité originale de VirusBarrier X5 réduit le temps nécessaire aux analyses de fichiers, ce qui renforce son côté non intrusif.

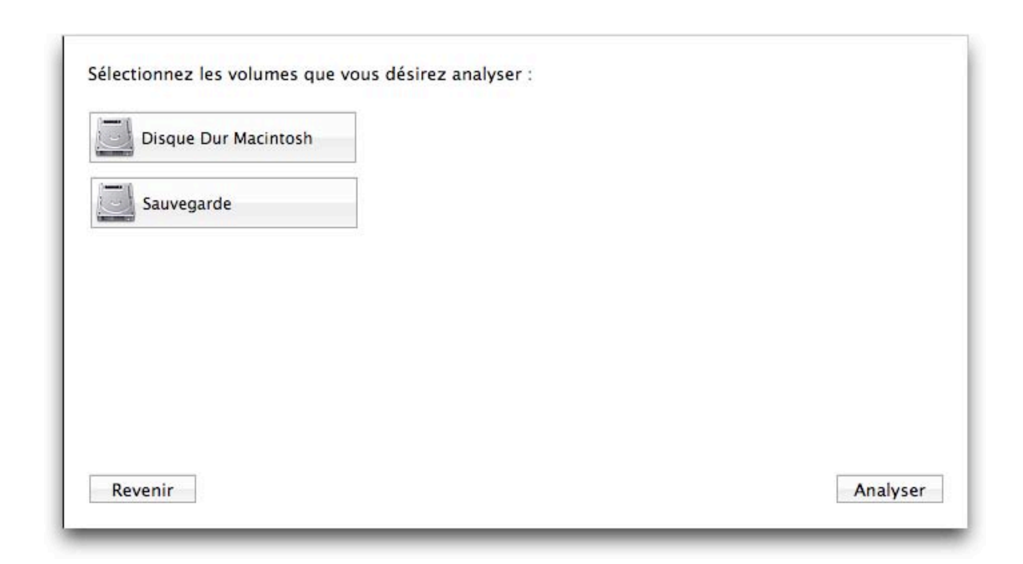
Vous pouvez lancer une analyse manuelle à tout moment. Il est conseillé de réaliser cette étape immédiatement après l'installation, pour s'assurer de l'absence de fichiers infectés. Ensuite, VirusBarrier X5 s'assure que tous les nouveaux fichiers sont exempts des virus.

Si vous n'avez pas lancé l'analyse complète dès l'installation, pour la lancer manuellement, ouvrez VirusBarrier X5 en double-cliquant sur son icône dans le dossier Applications. Vous pouvez réaliser l'analyse manuelle de tous les fichiers individuels ou des dossiers, par glisser-déposer soit sur l'icône du programme dans le Finder ou dans le Dock, soit sur l'Orbe quand VirusBarrier X5 est au premier plan.

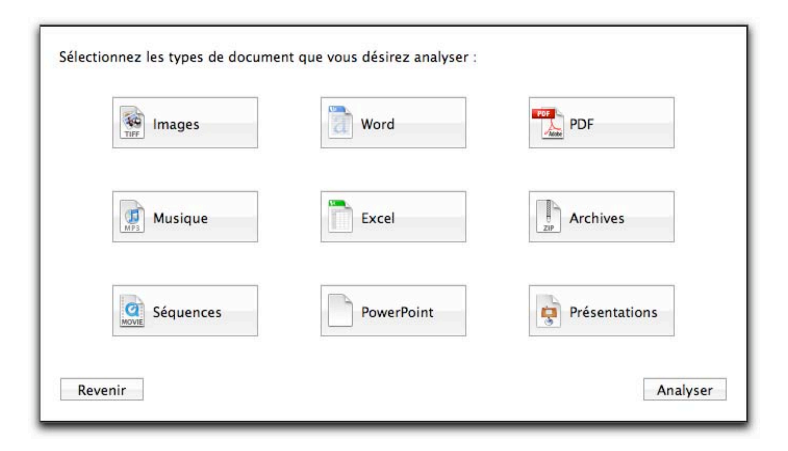
Cliquez sur le bouton **sélectionner** pour afficher les quatre boutons de sélection des éléments à analyser.



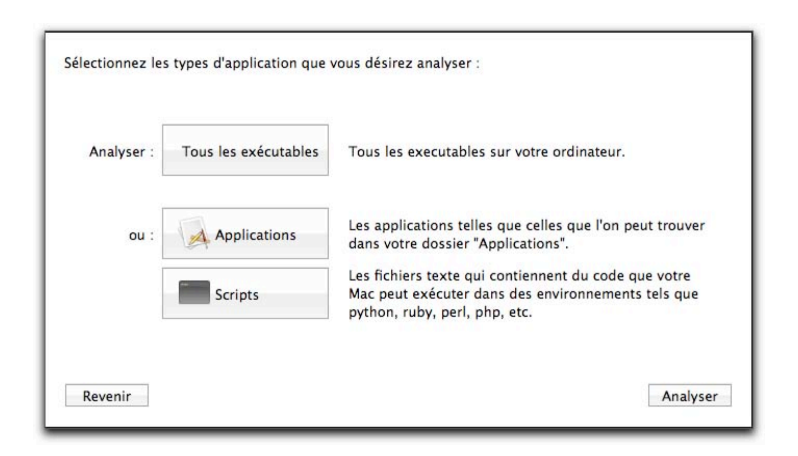
Le bouton **Disques durs** donne accès à la liste des disques durs connectés à votre Mac, ainsi que tout iPhone ou iPod touch connecté. Dans le cas ci-dessous, il y en a un seul, libellé Disque Dur Macintosh. Comme pour les quatre écrans de sélection, cliquez sur l'élément à analyser pour le sélectionner. Pour désélectionner un élément, cliquez à nouveau dessus. Cliquez sur Analyser pour commencer le processus d'analyse, ou sur Revenir pour retourner à l'écran de sélection.



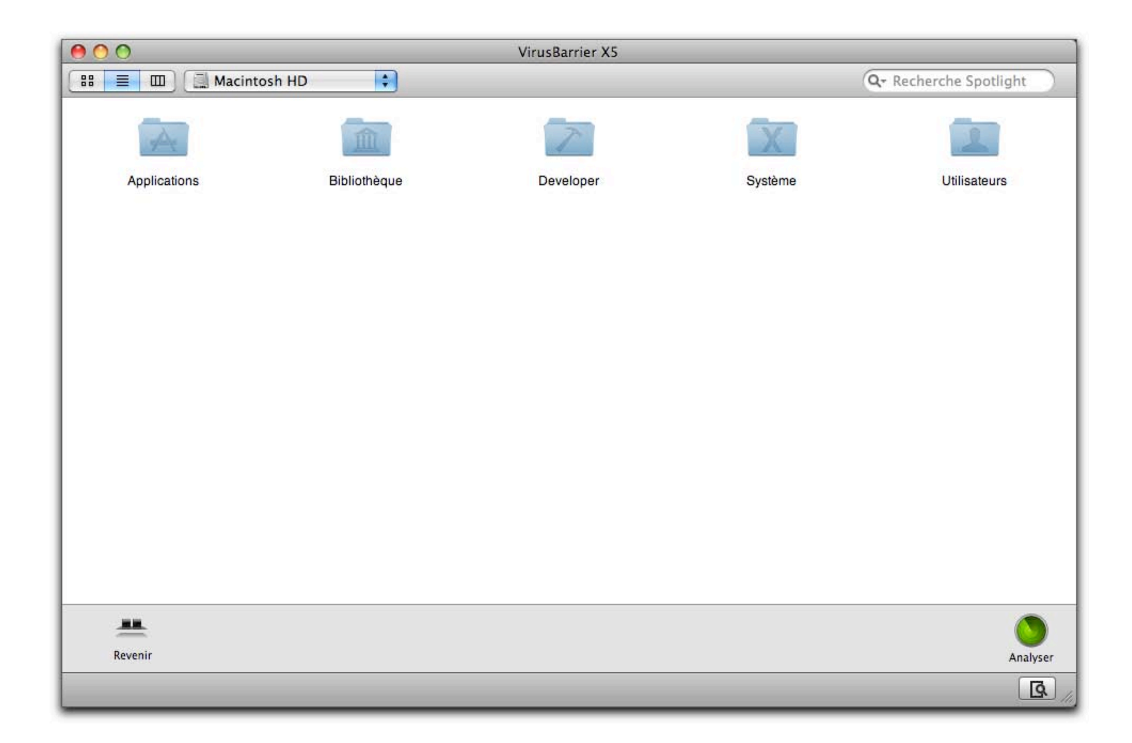
Le bouton **Documents** permet la sélection des éléments à analyser selon plusieurs types courants de fichiers, tels que PDF, Microsoft Word ou séquences. Comme ci-dessus, cliquez sur ceux que vous voulez analyser.



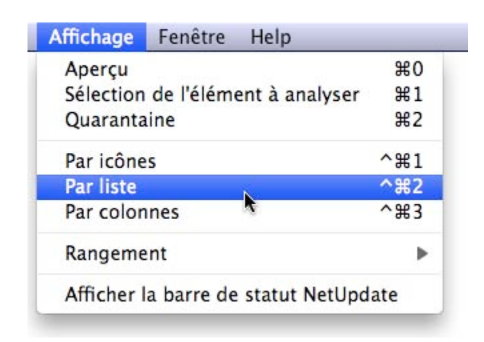
Le bouton **Applications** propose trois options d'analyse des fichiers exécutables, communément appelés applications ou programmes. Ces fichiers constituent un fort danger potentiel, vu que les virus qui se sont montés en "verrue" sur des applications, ou qui se sont fait passer pour des applications, pourraient avoir accès à toutes les ressources système de l'application elle-même. Les options sont d'analyser tous les exécutables trouvés par VirusBarrier X5, seulement ceux qui sont contenus dans votre dossier Applications, ou les scripts exécutables contenus dans des fichiers texte apparemment inoffensifs (comme ceux souvent présents dans les programmes écrits dans certains langages comme Perl et Python).



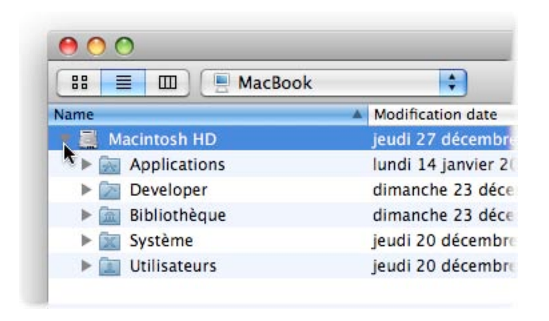
Enfin, le bouton **Naviguer** permet la sélection de n'importe quel groupe de fichiers et/ou de dossiers à analyser, quel que soit l'emplacement ou le type de fichier. En cliquant sur ce bouton, les fichiers sur votre Mac apparaissent en icônes dans une vue de type Finder.



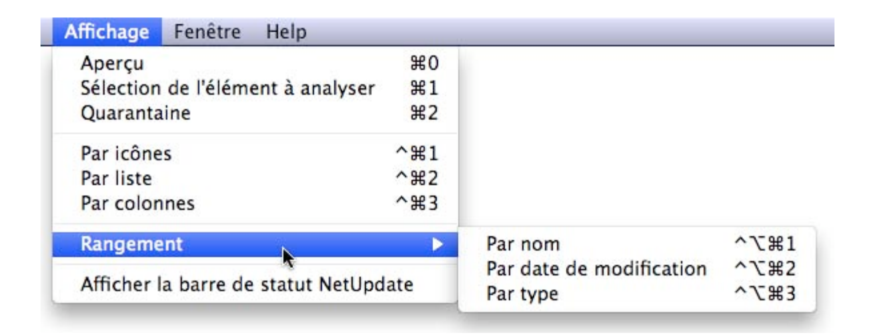
Comme dans le Finder, vous pouvez modifier l'affichage de vos fichiers pour voir une simple liste ou un navigateur de fichiers, en cliquant sur les boutons d'affichage en haut à gauche de la fenêtre. Vous pouvez également modifier l'affichage en choisissant la sélection voulue sous le menu Affichage (Par icônes, par liste ou par colonnes) ou en composant le raccourci clavier approprié (respectivement, Ctrl-Commande-1, Ctrl-Commande-2 ou Ctrl-Commande-3).



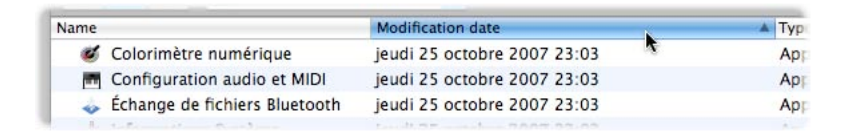
Quand l'affichage est par liste, vous pouvez voir les fichiers contenus dans un dossier en cliquant sur le triangle, à gauche du nom du dossier.



Pour les deux affichages par icônes et par liste, des options permettent de modifier l'ordre dans lequel les éléments apparaissent, sous le menu Affichage > Rangement : soit vous sélectionnez l'ordre de tri voulu (Par nom, par date de modification ou par type), soit vous composez le raccourci clavier approprié (respectivement, Ctrl-Option-Commande-1, Ctrl-Option-Commande-2 ou Ctrl-Option-Commande-3).



En affichage par liste, vous pouvez modifier l'ordre d'affichage en cliquant sur l'en-tête de la colonne choisie pour le tri. Ici, nous trions selon la date de modification, dans l'ordre ascendant. Pour trier une colonne dans l'ordre descendant, cliquez à nouveau sur l’en-tête de la colonne.



Quel que soit le mode d'affichage choisi, vous pouvez sélectionner plusieurs éléments en les rendant visibles, puis en maintenant la touche Commande enfoncée tout en cliquant sur un élément après l'autre. Quand la sélection est prête, cliquez sur **Analyser** pour lancer le processus.

Vous pouvez analyser tous les fichiers, les dossiers ou les volumes individuels, par glisser-déposer soit sur l'icône du programme, en fonctionnement en tâche de fond, soit sur l'Orbe, quand VirusBarrier X5 est au premier plan.

Si vous avez choisi **Compter les fichiers avant le scan** dans les préférences, VirusBarrier X5 compte le nombre total de fichiers à analyser, puis affiche le nombre de fichiers restant à analyser et le pourcentage d'analyse restant. De plus, le bord de l'Orbe est modifié pour indiquer visuellement l'avancement de l'analyse.



VirusBarrier X5 sait analyser les fichiers contenus dans des archives compressées. Lors de l'analyse des archives, l'affichage de l'Orbe est modifié pour indiquer que le programme traite une archive, et un bouton permet de passer l'analyse de cette archive, si elle est de taille importante et si vous êtes certain qu'elle soit sûre.



Si vous appuyez sur la touche Option quand une archive est affichée dans l'Orbe, le bouton Passer devient Afficher dans le Finder et vous pouvez voir l'emplacement de cette archive.

Lors de l'analyse d'un iPhone ou d'un iPod touch, VirusBarrier X5 copie tous les fichiers contenus vers le volume de démarrage de l'utilisateur, afin de vérifier leur sécurité. En cas de détection de maliciel ou de fichiers infectés, VirusBarrier X5 alerte l'utilisateur et propose de réparer ou de supprimer les fichiers infectés.

Vous pouvez arrêter l'analyse à tout moment en cliquant sur le bouton **stop**. Pour suspendre l'analyse, maintenez enfoncée la touche Option de votre clavier, vous constatez que le bouton **stop** affiche alors **pause**. Cliquez sur le bouton et l'analyse marque un temps de pause.



Pour reprendre l'analyse, cliquez sur ce bouton, qui affiche alors **continuer**.

Analyse en glisser-déposer

Vous pouvez analyser tout volume, dossier ou fichier par glisser-déposer sur l'Orbe. Un mot de passe administrateur peut être nécessaire, si vous n'avez pas les permissions nécessaires pour l'accès aux fichiers contenus dans l'élément que vous faites glisser sur l'Orbe.



Le résultat est le même en faisant glisser-déposer le volume, dossier ou fichier sur l'icône du programme VirusBarrier X5 dans le Finder.



Enfin, vous pouvez glisser-déposer les éléments à analyser sur l'icône VirusBarrier X5 dans le Dock.



Dès que vous relâchez l'élément, VirusBarrier X5 démarre l'analyse, comme pour toute analyse manuelle.

Analyse planifiée

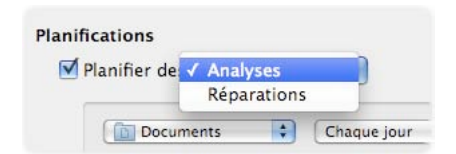
VirusBarrier X5 peut être réglé pour fonctionner automatiquement à des dates préfixées. Cliquez sur la flèche dans l'instrument **planifications** pour ouvrir les préférences des planifications.



Les réglages en haut de la fenêtre des préférences contrôlent plusieurs fonctions dont nous discuterons au chapitre 6, **Préférences de VirusBarrier X5**. Voyons la section **Planifications** au bas de la fenêtre.



Pour activer la planification, cochez la case **Planifier des**. Dans le menu déroulant adjacent, vous pouvez choisir si VirusBarrier X5 va simplement analyser vos fichiers au moment fixé, ou s'il va également apporter les réparations possibles, en cas de détection de fichiers infectés.

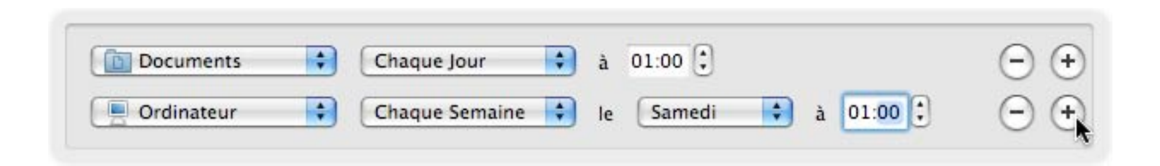


Sous ces réglages, un sélecteur de planification permet de préciser le dossier à analyser et le moment de l'analyse. Le premier menu déroulant liste les dossiers que vous allez très probablement analyser, y compris votre dossier de départ et votre dossier Documents. Le choix par défaut, **Ordinateur**, demande à VirusBarrier X5 d'analyser tous les dossiers pour tous les utilisateurs sur votre Mac.

Le second menu déroulant permet de choisir la fréquence de l'opération, quotidienne ou hebdomadaire. Si vous sélectionnez Chaque jour, vous pouvez choisir l'heure voulue ; sélectionnez Chaque semaine et vous choisirez également le jour préféré.



Vous pouvez créer des planifications en plusieurs segments, par exemple, pour analyser votre dossier Documents chaque nuit, et votre ordinateur en entier une fois par semaine. Pour cela, cliquez sur le bouton + à droite de l'élément de planification : un autre élément va s'ajouter au-dessous. Apportez les modifications nécessaires à cet élément. Ajoutez ainsi autant d'éléments de planification que nécessaire ; pour en supprimer un, cliquez sur le bouton – à côté de l'élément.



L'ordre des éléments de planification n'est pas important ; si vous prévoyez que deux analyses soient effectuées au même moment, elles se produiront simultanément.

Quand vous avez terminé, le nombre d'éléments de planification en attente apparaît dans l'instrument **planifications** sur l'interface principale de VirusBarrier X5. Pour désactiver toutes les planifications en attente, revenez à l'écran des préférences de planification et décochez le bouton **Planifier des**.



Analyse des e-mails

VirusBarrier X5 sait analyser les courriers électroniques entrants et sortants. Toutes les pièces jointes infectées sont ainsi identifiées dès l'arrivée, avant qu'elles n'aient pu nuire à un autre correspondant, dont l'attention est peut-être retenue par d'autres messages. L'analyse des messages sortants est importante pour les autres ordinateurs.

VirusBarrier X5 analyse les messages sortants et leurs pièces jointes, assurant que vous n'envoyez pas de virus à vos correspondants.

VirusBarrier X5 peut uniquement analyser les messages venant des programmes qui stockent leurs messages en fichiers individuels, comme Apple Mail. Cependant, quand vous ouvrez ou enregistrez des pièces jointes, VirusBarrier X5 analyse tous les fichiers, quel que soit leur programme d'origine.

Alertes

Bien que VirusBarrier X5 sache réaliser des analyses manuelles, comme nous venons de le voir, la plupart des utilisateurs préfèrent qu'il travaille en tâche de fond. Il propose alors diverses alertes en cas de détection de fichiers infectés.

En cas de détection, si vous avez réglé VirusBarrier X5 pour l'analyse, et non pas la réparation automatique des fichiers infectés, une alerte apparaît.



Si vous analysez les éléments par glisser-déposer sur l'Orbe de VirusBarrier, l'aspect de l'alerte est différent :



En cliquant sur **Afficher dans le Finder**, une fenêtre de Finder présente l'emplacement du fichier sur votre disque dur. Si vous souhaitez que VirusBarrier X5 répare le fichier, cliquez sur **Réparer** ; pour l'isoler, cliquez sur **Mettre en quarantaine**. Pour en savoir plus sur la zone de quarantaine, reportez-vous au paragraphe correspondant dans ce chapitre. Si vous voulez ne rien faire, cliquez sur **Ignorer**, et le fichier n'est pas réparé.

ATTENTION : Le fait d'ignorer les alertes de virus peut être risqué ! Choisissez de ne pas réparer seulement si vous êtes bien sûr de votre fait !

Si vous ne répondez pas à une alerte dans le délai d'une minute, VirusBarrier X5 place le fichier dans la zone de quarantaine. Vous pouvez vérifier les fichiers dans la zone de quarantaine ultérieurement, pour décider du mode d'action. Consultez le paragraphe Zone de quarantaine, dans ce chapitre.

Pour en savoir plus, reportez-vous au chapitre 6, **Préférences de VirusBarrier X5**.

Zone de confiance

VirusBarrier X5 offre l’option d'ajouter les fichiers, dossiers ou volumes dans une zone de confiance. VirusBarrier X5 fait confiance à tous les fichiers que vous ajoutez dans cette zone et il ne les analyse pas. Il est conseillé de réserver cette zone aux fichiers sûrs qui ont déjà été analysés par VirusBarrier X5.

Pour ajouter des éléments à la zone de confiance, ouvrez les préférences de VirusBarrier X5 et cliquez sur l'icône **Scanner**. Dans la section **Zone de confiance**, vous pouvez définir des fichiers, dossiers ou volumes que le scanner temps réel de VirusBarrier X5 ne va pas analyser. Cependant, VirusBarrier X5 vérifie ces éléments quand vous effectuez des analyses manuelles de votre Mac.

Pour ajouter un élément à la zone de confiance, cliquez sur le bouton +, naviguez vers un élément, puis cliquez sur Choisir. Vous pouvez faire glisser des fichiers ou des dossiers du Finder vers ce champ. Note : en ajoutant un dossier ou un volume, vous indiquez à VirusBarrier X5 de faire confiance à *tous* les fichiers contenus dans l'élément sélectionné, ainsi que tous les sous-dossiers qu'il renferme. Pour supprimer un élément de la zone de confiance, cliquez dessus pour le sélectionner, puis sur le bouton -.

Le menu contextuel sert également à ajouter des éléments à la zone de confiance. Consultez la section correspondante dans ce manuel, pour plus d’informations.

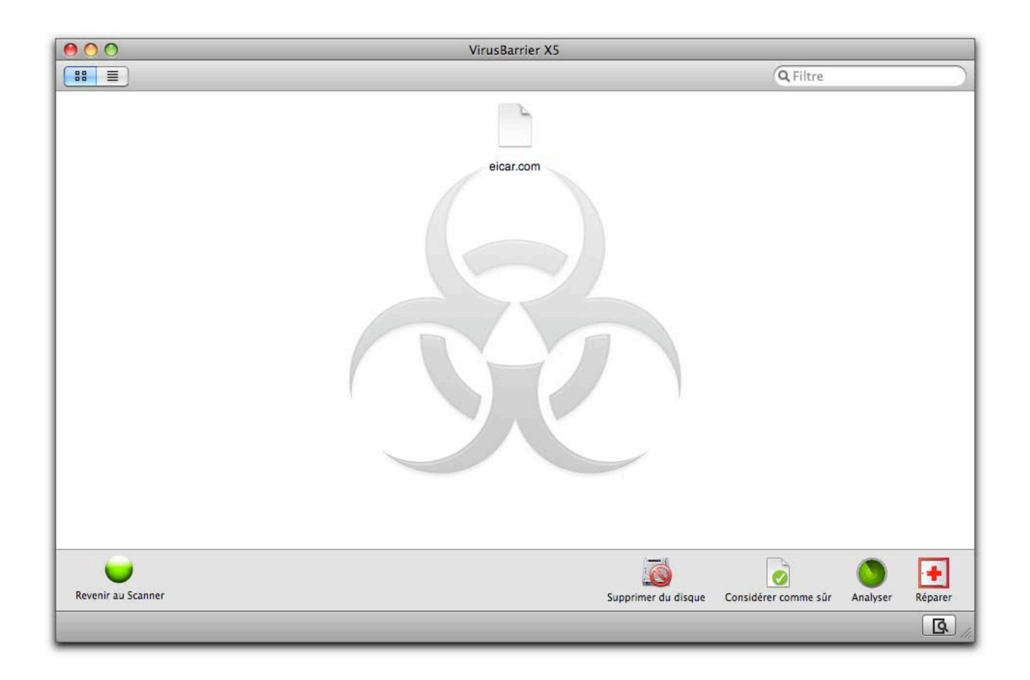
Zone de quarantaine

Si vous ne voulez pas réparer les fichiers automatiquement, vous pouvez régler VirusBarrier X5 pour qu'il les place dans une zone spéciale de quarantaine. Quand les fichiers sont mis en quarantaine, ils ne peuvent être ni ouverts ni lus, ce qui assure qu'ils ne puissent pas infecter votre Mac. Cette fonction est utile aux administrateurs qui veulent vérifier les fichiers avant de lancer les fonctions de réparation de VirusBarrier X5.

Comme indiqué plus haut, VirusBarrier X5 place le fichier dans la zone de quarantaine si vous ne répondez pas à une alerte dans le délai d'une minute. Vous pouvez ensuite vérifier les fichiers, pour décider du mode d'action. L'instrument **quarantaine** indique le nombre de fichiers isolés dans cette zone.



Pour afficher le contenu de la zone de quarantaine, cliquez sur la flèche dans l'instrument. Une fenêtre présente les fichiers contenus dans la zone de quarantaine, ainsi que plusieurs boutons permettant d'agir sur ces éléments.



Vous pouvez modifier l'affichage des fichiers dans la zone de quarantaine pour voir une simple liste ou des icônes ; pour cela, cliquez sur l'un des boutons d'affichage en haut à gauche de la fenêtre.

Pour agir sur l'un des fichiers, sélectionnez-le, puis cliquez sur l'un des quatre boutons en bas à droite de la fenêtre.



Les choix sont les suivants :

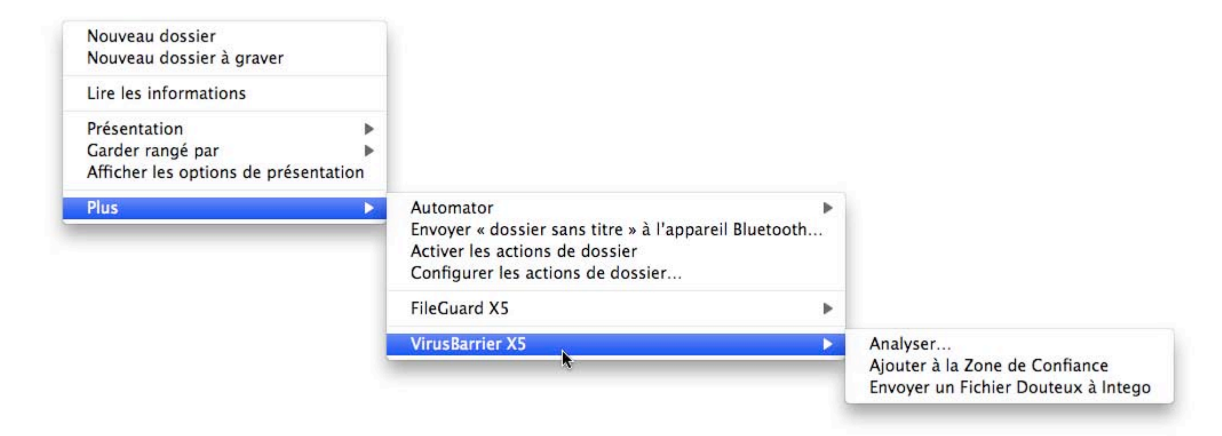
- **Supprimer du disque** supprime le fichier de votre Mac.
- **Considérer comme sûr** indique à VirusBarrier X5 que vous pensez que ce fichier n'est pas infecté. Cela peut être le cas pour les faux positifs. Cependant, soyez *très vigilant* en cliquant ce bouton ; il faut être certain que le fichier soit sûr. Sinon, il risque d'infecter tout votre Mac.
- **Analyser** indique à VirusBarrier X5 d'analyser le fichier à nouveau. Vous pouvez procéder ainsi dans le cas de fichiers qui ont été ajoutés automatiquement à la zone de quarantaine, pour lesquels vous voulez savoir ce qui les a infectés.
- **Réparer** indique à VirusBarrier X5 de réparer le fichier, en éliminant le virus.

Si vous affichez la zone de quarantaine en mode liste, une colonne Virus précise les virus ayant infecté vos fichiers.

Menu contextuel de VirusBarrier X5

VirusBarrier X5 offre l'option de fonctionner directement à partir du Finder sous Mac OS X, à l'aide d'un menu contextuel.

Pour cela, il suffit de Ctrl-cliquer ou de cliquer du bouton droit de la souris sur un élément – fichier, dossier ou volume – et un menu contextuel apparaît. Sous Mac OS X 10.5, Leopard, le menu VirusBarrier X5 apparaît sous le menu Plus, alors que des versions antérieures de Mac OS X présentent immédiatement ce menu.



Le menu contextuel propose les actions suivantes :

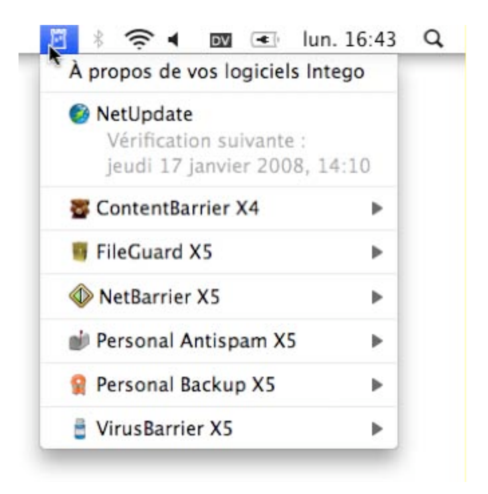
- Vous pouvez analyser l'élément sélectionné (et le réparer, selon les réglages du programme).
- Vous pouvez ajouter l'élément à la Zone de Confiance.
- Vous pouvez soumettre une copie de l'élément à Intego en choisissant **Envoyer un fichier douteux à Intego**. Pour cela, vous devez configurer les réglages d'e-mail. Si vous ne l'avez pas fait dans les préférences d'historique de VirusBarrier X5, un dialogue vous demande les informations nécessaires. Cette option est très utile dans le cas de fichiers présumés infectés par des virus nouveaux ou non reconnus. Si vous choisissez cette option, les experts en virus d'Intego peuvent étudier le fichier et produire les définitions de virus nécessaires à la protection des systèmes utilisateurs.

Menu Intego

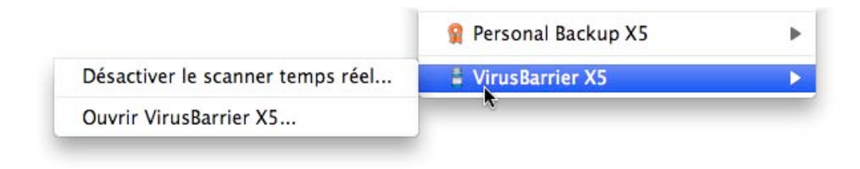
VirusBarrier X5, comme tous les autres logiciels Intego, installe un menu spécifique dans la barre de menus, appelé le menu Intego. Son icône est une petite tour, comme dans le logo Intego.



Cliquez sur l'icône du menu Intego pour afficher le menu présentant tous vos logiciels Intego :



Vous pouvez activer ou désactiver le scanner temps réel, et ouvrir VirusBarrier X5 depuis le menu Intego.



Pour en savoir plus sur ce menu, reportez-vous au Manuel de Démarrage Intego.

5 – Comprendre le résultat d'analyse

Résultat d’analyse

Lors d'une analyse manuelle, VirusBarrier X5 vous informe de la détection de fichiers infectés par des virus connus. En cas de détection de fichiers infectés, l’Orbe de VirusBarrier X5 devient rouge. Si VirusBarrier X5 découvre des fichiers corrompus, l'Orbe devient orange. En cas de détection de fichiers infectés et de fichiers corrompus, l'Orbe va clignoter en rouge et orange. VirusBarrier X5 vous alerte également, en fonction des options d’alerte définies dans les Préférences. Pour en savoir plus sur les options d’alerte, consultez le chapitre 6, **Préférences de VirusBarrier X5**.



Vous pouvez mieux comprendre les résultats d'analyse en vérifiant les historiques de VirusBarrier X5.

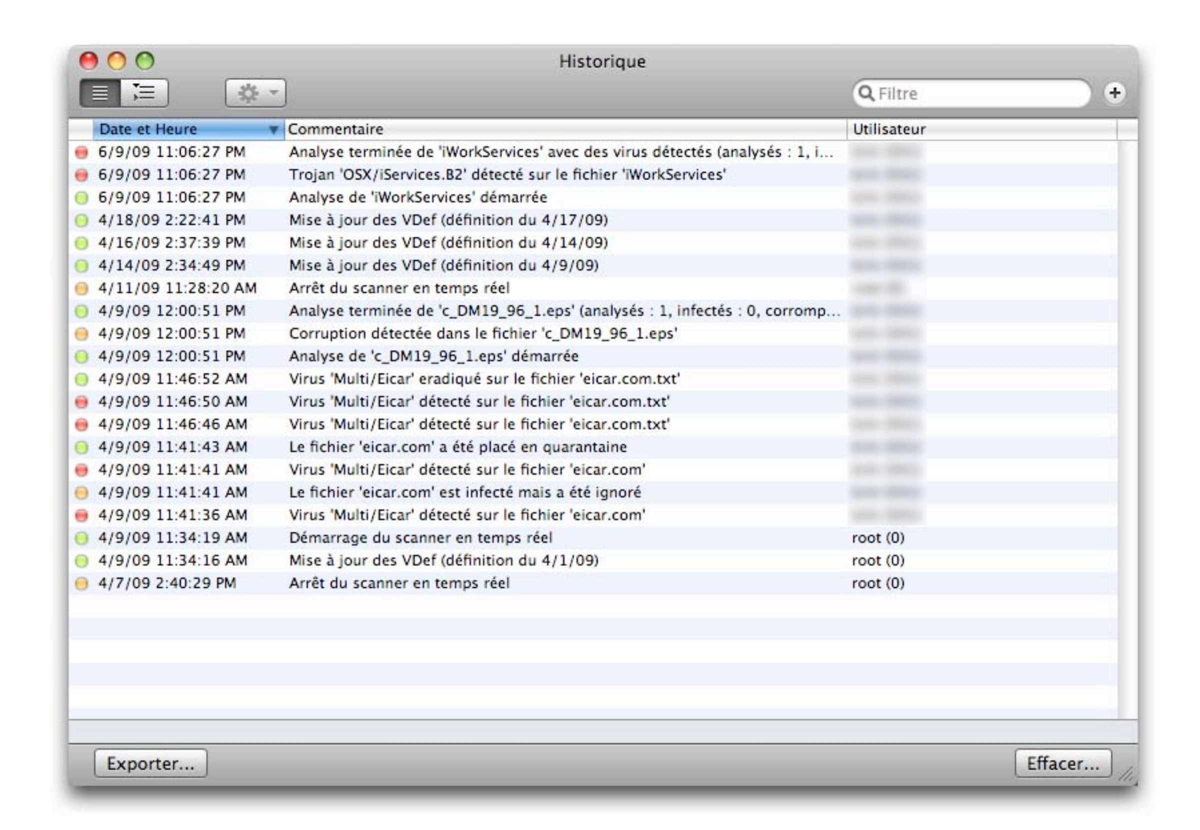
Historiques de VirusBarrier X5

Pour consulter les opérations que VirusBarrier X5 a réalisées depuis sa première installation, cliquez sur l'icône en bas à droite de l'interface principale pour révéler la fenêtre de l'historique.

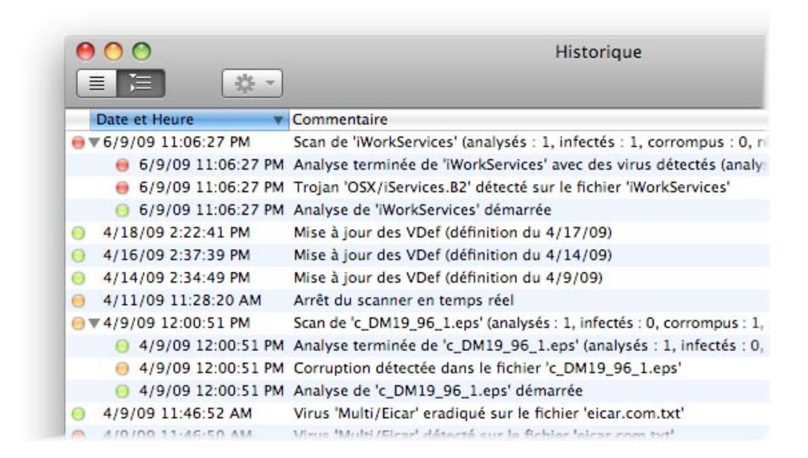


L'historique apparaît automatiquement si VirusBarrier X5 trouve des fichiers infectés, et si vous avez sélectionné cette option dans les préférences d'historique (Consulter le chapitre 6, **Préférences de VirusBarrier X5**). Vous pouvez également ouvrir l'historique en choisissant le menu Intego > VirusBarrier X5 > Ouvrir l’historique.

Voilà un exemple d'historique.



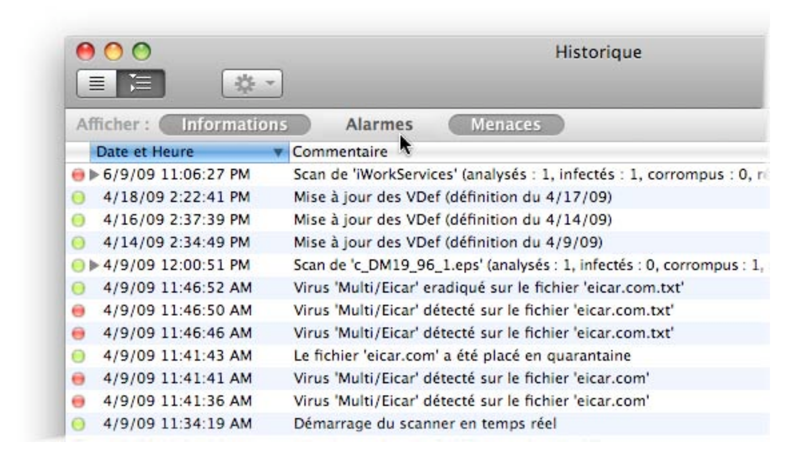
Vous pouvez afficher les informations de l'historique de deux façons. Dans l'exemple ci-dessus, les entrées sont présentées dans un ordre linéaire, chacune sur une ligne. En cliquant sur le second bouton en haut à gauche de la fenêtre, les entrées vont s'afficher en ordre hiérarchique, où les triangles regroupent des entrées reliées :



L'historique indique chaque fois que :

- Vous démarrez une analyse
- Vous annulez une analyse en cours d'exécution
- Vous démarrez ou arrêtez l'analyse en temps réel
- VirusBarrier X5 termine une analyse, avec ses résultats
- VirusBarrier X5 découvre un virus
- VirusBarrier X5 découvre un fichier corrompu
- VirusBarrier X5 répare un fichier infecté
- Des fichiers sont ajoutés ou supprimés de la zone de quarantaine.
- Des définitions de virus sont mises à jour

Les pastilles de couleur dans la colonne à gauche indiquent les types d'entrées dans l'historique. Les pastilles vertes indiquent des informations, comme le démarrage de l'analyse en temps réel ou la mise à jour de définitions de virus. Les pastilles oranges sont pour des alarmes, comme l'arrêt de l'analyse en temps réel. Les pastilles rouges indiquent des menaces, comme en cas de détection de fichiers infectés ou corrompus. Le statut des analyses nomme clairement les fichiers, dossiers ou volumes sélectionnés et les problèmes détectés. Vous pouvez choisir d'afficher seulement certains types d'informations en cliquant sur l'icône + à droite de la fenêtre de l'historique, puis en cliquant sur l'un des trois boutons de type d'historique pour cacher ou afficher leurs entrées.

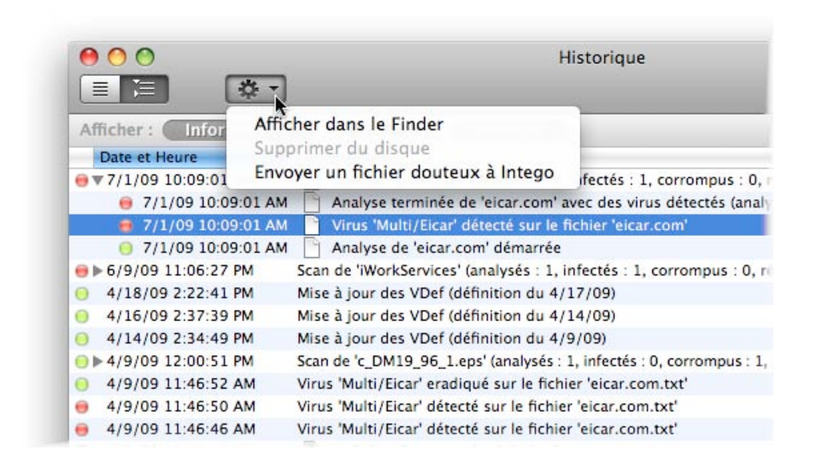


Si des maliciels sont détectés, ils sont listés selon quatre catégories :

- Virus
- Backdoor
- Cheval de Troie
- Exploit

Certaines lignes de l'historique sont relativement longues, et ne sont pas complètement visibles dans la fenêtre. En cliquant et en faisant glisser le coin inférieur droit, vous pouvez modifier la taille de l’ensemble de la fenêtre ; vous pouvez cliquer et faire glisser les en-têtes de colonne pour afficher plus de texte. Pour trier selon le contenu d'une colonne, cliquez une fois sur son en-tête ; un second clic fait basculer le tri de la colonne entre les ordres ascendant (1, 2, 3) et descendant (3, 2, 1).

Vous pouvez réaliser des actions sur certaines entrées de l'historique en les sélectionnant et en cliquant sur le bouton Action dans la barre d'outils de la fenêtre d'historique, ou par Control-clic ou clic droit. Un menu contextuel propose alors trois options :



- Afficher dans le Finder : cette option ouvre une fenêtre du Finder avec le fichier sélectionné ; vous pouvez alors l'effacer ou lui appliquer d'autres actions.
- Supprimer du disque: cette option n'est disponible que pour les fichiers corrompus, qui sont alors effacés de votre disque.
- Envoyer un fichier douteux à Intego : choisissez cette option pour envoyer tous fichiers douteux à Intego, et nous les examinerons.

Vous pouvez filtrer les résultats de recherche en tapant du texte dans le champ de recherche situé dans la barre des menus de la fenêtre. Au fil de la frappe, l'historique se réduit et n'affiche que les entrées contenant la chaîne recherchée.

Vous pouvez copier des éléments de l'historique en les sélectionnant et en appuyant sur Commande-C ; vous pouvez ensuite les coller dans une autre application, si nécessaire.

Vous pouvez effacer des éléments de l'historique en les sélectionnant et en appuyant sur Effacer. Vous pouvez effacer tout l'historique, en cliquant sur le bouton Effacer....

VirusBarrier X5 et la ligne de commande

VirusBarrier X5 offre l'option d'analyser des fichiers et des volumes depuis la ligne de commande. L'exemple suivant décrit la mise en oeuvre de cette commande.

```
/Library/Intego/virusbarrier.bundle/Contents/Resources/virusbarriers
[-rtcCaz] <chemin d'accès à scanner> [<chemin d'accès du répertoire courant>]
```

Les options suivantes sont disponibles :

```
-r:    Répare les fichiers infectés.
-t:    Utilise le mode Turbo ; ne scanne que les fichiers qui n'ont pas été
       modifiés depuis le scan précédent.
-c:    Compte les fichiers avant de scanner.
-C:    Compte les fichiers, mais ne les scanne pas.
-a:    Scanne tous les fichiers, y compris ceux liés à d'autres volumes par
       des liens symboliques (ou à d'autres points de montage dans /Volumes)
-z:    Scanne les archives compressées (y compris celles dans les pièces
       jointes aux e-mails)
```

<chemin d'accès à scanner> : Ceci est obligatoire ; il peut s'agir d'un chemin relatif ou absolu.

[<chemin d'accès du répertoire courant>]: Ceci est optionnel ; il s'agit du répertoire courant si on utilise un chemin d'accès relatif dans le premier argument.

Exemple :

```
/Library/Intego/virusbarrier.bundle/Contents/Resources/virusbarriers
-tacz /
```

Cette commande scanne tous les volumes pour lesquels l'utilisateur a les droits de lecture. Il scanne les archives et compte le nombre de fichiers à scanner avant de lancer le scan. Si vous précédez la commande par sudo vous pouvez scanner tous les fichiers.

Vous pouvez également créer des alias pour simplifier le lancement de cette commande.

Si vous utilisez bash :

```
alias
vbscan=/Library/Intego/virusbarrier.bundle/Contents/Resources/virusbarriers
```

Si vous utilisez tcsh :

```
alias vbscan
/Library/Intego/virusbarrierd.bundle/Contents/Resources/virusbarriers
```

Avec ces alias vous pouvez lancer la commande en exemple comme suit :

```
vbscan -tacz /
```

6 – Préférences de VirusBarrier X5

Préférences de VirusBarrier X5

VirusBarrier X5 est conçu pour travailler sans se faire remarquer, en tâche de fond, dès son installation. Il dispose de nombreuses options pour contrôler le choix des fichiers à analyser, le mode d'analyse, et le mode d'affichage des résultats. Vous pouvez régler les options du programme dans sa fenêtre des préférences, soit en choisissant VirusBarrier X5 > Préférences..., soit en appuyant sur Commande-virgule.

La fenêtre des préférences est divisée en quatre panneaux : Générales, Scanner, Planification et Evénements, et Historiques.

Préférences générales



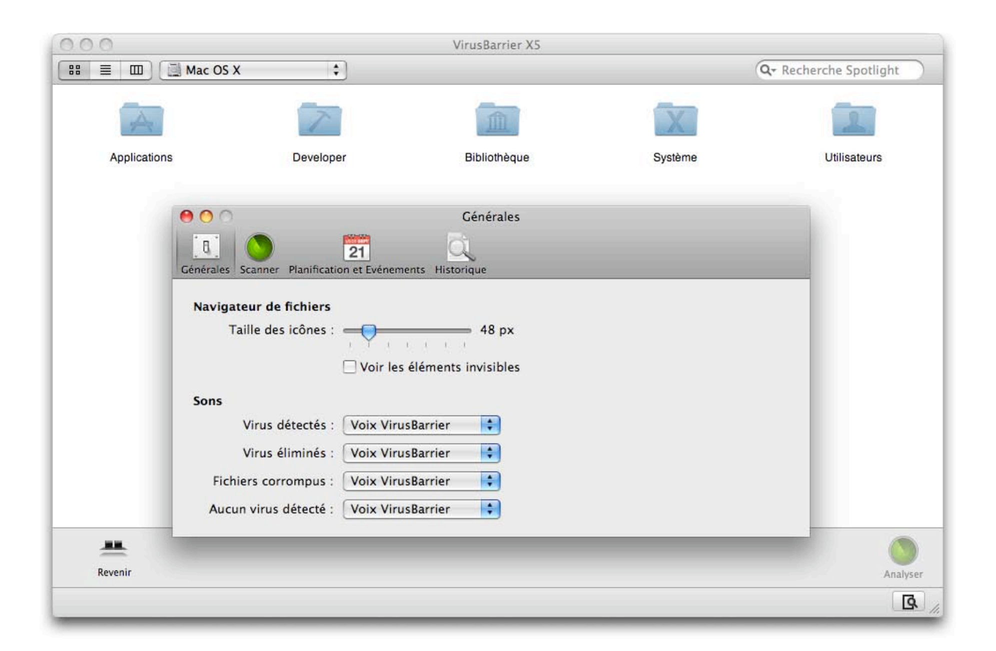
La première section du panneau contrôle l'apparence du programme ; en bas, l'interface sonore du programme. Voilà une explication de chaque option :

Le curseur **Taille des icônes** permet de choisir la taille des icônes, en pixels, quand la navigation se fait en affichage d'icônes (Affichage > par icônes). (Les modifications de ce réglage n'ont pas d'effet lors de l'affichage en mode liste ou colonne.)

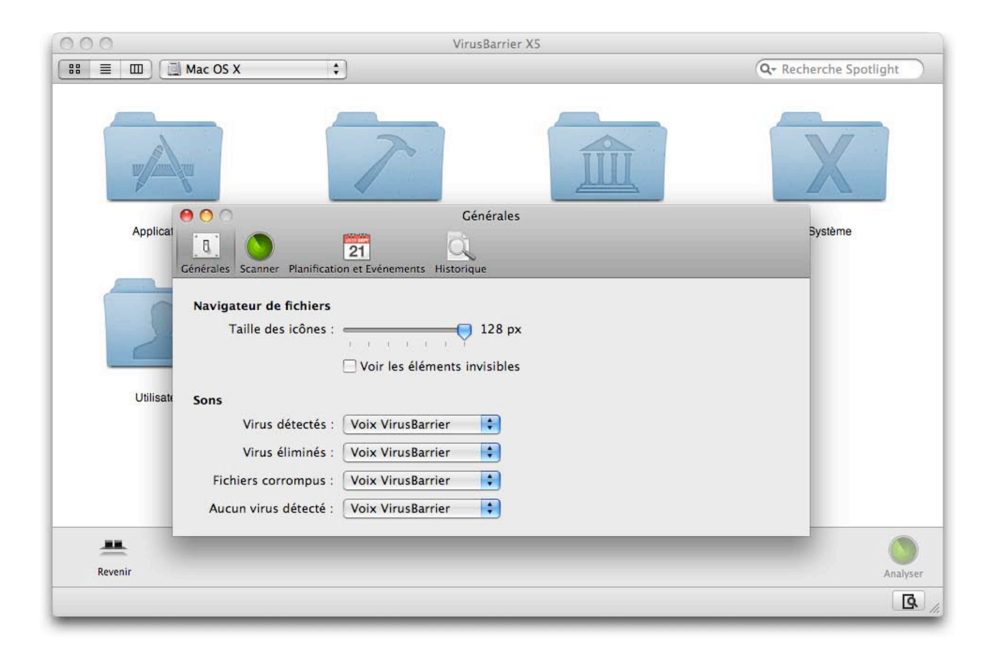
La seconde option, **Voir les éléments invisibles**, affiche les fichiers que Mac OS X tient habituellement cachés. Ce sont généralement des fichiers nécessaires au fonctionnement correct de votre Mac, qui ne devraient pas être modifiés. Les virus et autres maliciels peuvent se cacher

dans des fichiers invisibles, il est donc très important de les analyser. Cependant, vous n'avez pas besoin de les rendre visibles pour les analyser : quand vous analysez un dossier, VirusBarrier X5 analyse chacun de ses éléments, y compris les invisibles.

Voici l'affichage par icônes, en réglage par défaut avec des icônes de 48 x 48 pixels et sans aucun fichier invisible :



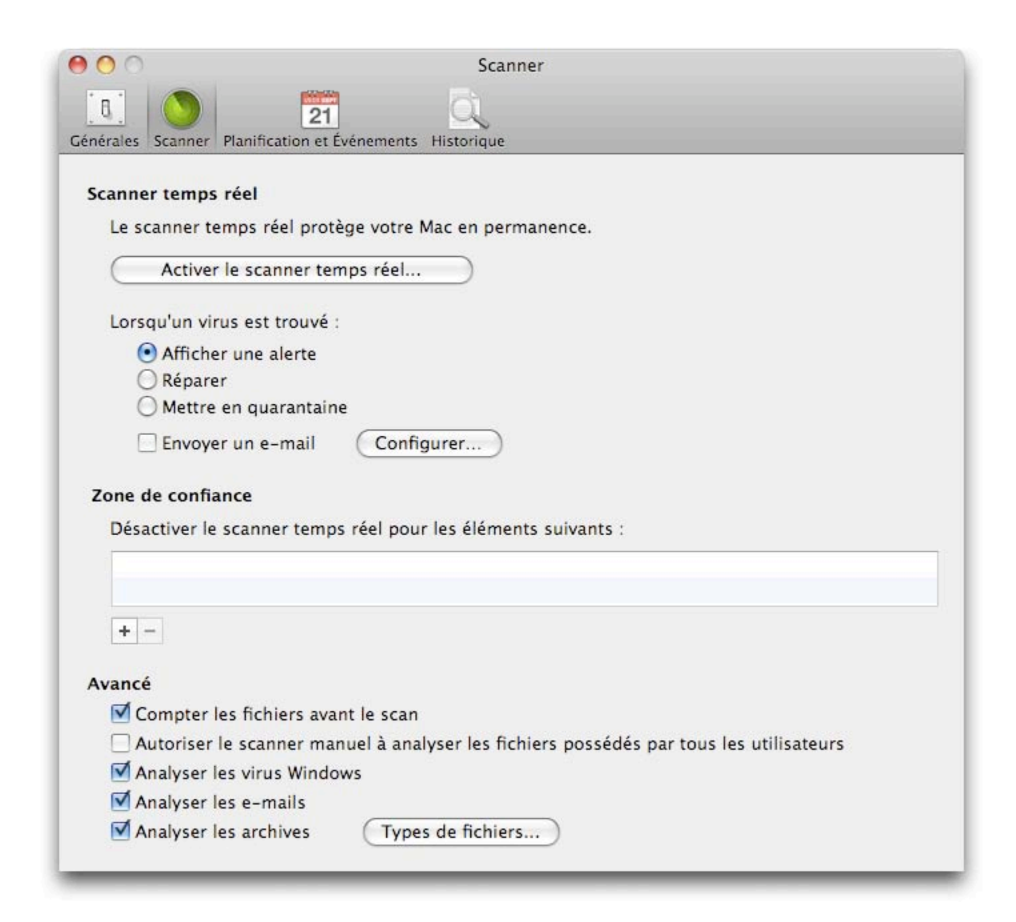
Voilà le même dossier, avec des icônes plus grandes et les éléments invisibles affichés :



Note : la zone de quarantaine affiche toujours les éléments invisibles, quel que soit le réglage dans ces préférences.

La section **Sons** permet de contrôler l'interface sonore en cas de détection ou d'élimination d'un virus, lors de la découverte d'un fichier corrompu, ou quand VirusBarrier X5 termine une analyse sans trouver de virus. Par défaut, la Voix VirusBarrier annonce ces événements : vous pouvez les écouter en cliquant sur le menu déroulant approprié et en re-sélectionnant "Voix VirusBarrier". Vous pouvez modifier chaque son dans ce menu. Pour désactiver un des sons, il suffit de choisir **Aucun** dans le menu déroulant.

Préférences de scanner



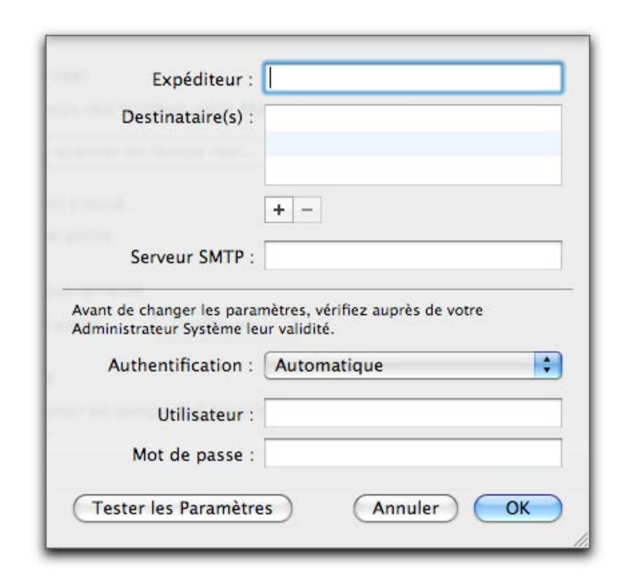
Le panneau des préférences de Scanner contrôle le comportement de VirusBarrier X5 lors des analyses en tâche de fond. Comme le scanner en temps réel est très discret, VirusBarrier X5 propose plusieurs méthodes de notification en cas de découverte d'un virus.

Pour activer le scanner en temps réel, cliquez sur le bouton **Activer le scanner temps réel...** ; pour le désactiver, cliquez sur le bouton **Désactiver le scanner temps réel...**. En fonctionnement normal, vous n'avez pas besoin de désactiver le scanner ; cela est utile uniquement en cas de dépannage quand vous avez un problème sur votre Mac. Note : vous pouvez lancer et arrêter le scanner temps réel depuis le menu Intego, en sélectionnant VirusBarrier X5 > Désactiver / Activer le scanner temps réel.

Le contrôle suivant permet de préciser le mode d'action de VirusBarrier X5 quand il trouve un virus. Les options sont les suivantes :

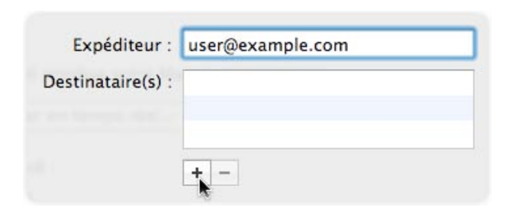
- **Afficher une alerte**. C'est l'option adéquate quand vous effectuez une analyse de virus sur un Mac "en surveillance" – c'est-à-dire, que vous surveillez suffisamment de près pour voir l'alerte quand elle surgit. Note : si vous ne répondez pas à une alerte dans le délai d'une minute, VirusBarrier X5 met les fichiers infectés dans la zone de quarantaine.
- **Réparer**, qui tente d'éliminer le virus.
- **Mettre en quarantaine**, qui assure que le fichier ne peut être ni ouvert ni lu. Consultez la section Zone de quarantaine au chapitre 4, **Analyse de votre Mac avec VirusBarrier X5**.

De plus, vous pouvez choisir l'envoi de message par VirusBarrier X5 quand il découvre un virus. Pour cela, cochez la case **Envoyer un e-mail**, puis cliquez sur le bouton **Configurer...** adjacent.



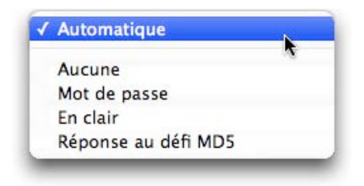
Vous devez entrer les adresses de l'expéditeur, du (ou des) destinataires et du serveur SMTP. Vous pouvez envoyer le message à plusieurs destinataires. Pour entrer les adresses, cliquez sur le bouton +. Une fausse adresse apparaît, comme indiqué ci-dessous. Remplacez la fausse adresse par l'adresse réelle du destinataire que vous avez choisi pour recevoir le message d'alerte. Pour éliminer des destinataires, utilisez le bouton –.

Vous devez saisir les adresses de l'expéditeur et du (ou des) destinataire(s), ainsi que le serveur SMTP. Puis, vous devez entrer un nom d'utilisateur et un mot de passe que votre serveur de messagerie va accepter. Plusieurs destinataires peuvent recevoir les messages. Pour ajouter un destinataire, cliquez sur le bouton +. Pour éliminer un destinataire, cliquez sur le bouton -.



La partie basse du dialogue des Préférences d'e-mail traite d'options avancées, dont VirusBarrier X5 peut avoir besoin pour envoyer un message.

Le menu déroulant indique les divers types d'authentification d'e-mail considérés.



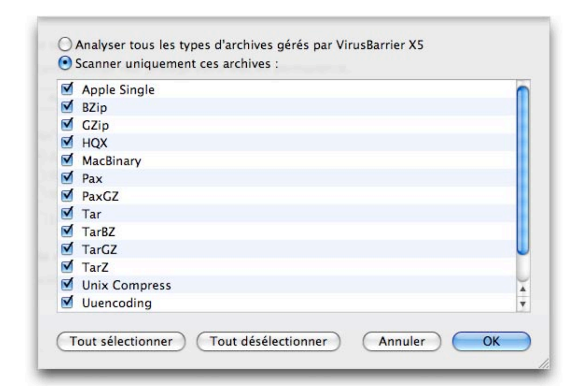
Il est conseillé d'utiliser les mêmes critères (authentification, nom d'utilisateur et mot de passe) que ceux utilisés dans votre programme de messagerie habituel, si vous administrez votre propre système. Par ailleurs, si vous avez un administrateur de système, il est conseillé de vérifier, auprès de cette personne, les réglages à mettre en œuvre dans ce contexte. Si vous ne connaissez pas le type d'authentification utilisé, sélectionnez **Automatique**.

Quand c'est terminé, vous pouvez confirmer que le message va passer en cliquant sur le bouton **Tester les paramètres**. Il se peut que vous ayez à attendre plusieurs secondes pour que votre serveur de messagerie réponde ; quand c'est terminé, les résultats apparaissent dans un dialogue.

La section suivante des préférences permet d'exclure des analyses en temps réel certains fichiers, dossier et volumes, en les ajoutant à la zone de confiance. (Consultez la section Zone confiance au chapitre 4, **Analyse de votre Mac avec VirusBarrier X5**, pour en savoir plus sur cette zone.)

Le bas du panneau des préférences du scanner donne accès à six réglages avancés, qui concernent les analyses manuelles et automatiques.

- **Compter les fichiers avant le scan** : VirusBarrier X5 compte le nombre de fichiers à analyser, ce qui donne alors une information plus précise sur la durée de l'analyse, par l'affichage dans l'Orbe du nombre de fichiers et du pourcentage d'avancement, lors d'une analyse manuelle.
- **Autoriser le scanner manuel à analyser les fichiers possédés par tous les utilisateurs :** VirusBarrier X5 va aller au-delà du compte utilisateur qui est connecté au début de l'analyse, pour scanner les fichiers sur votre Mac, y compris ceux appartenant à d'autres utilisateurs. Si vous cochez cette option, vous devez immédiatement taper un mot de passe administrateur ; si vous n'avez pas ce mot de passe, la case revient à son état décoché. Si vous ne cochez pas cette option et VirusBarrier X5 détecte un fichier infecté appartenant à un utilisateur différent ou au système, la fenêtre d'alerte et de zone de quarantaine de VirusBarrier X5 affiche une icône de crayon barré, indiquant que vous devrez saisir un nom et un mot de passe d'administrateur pour réaliser toute action sur le fichier.
- **Analyser les virus Windows** : VirusBarrier X5 surveille les virus qui affectent Windows. Bien que ces fichiers ne risquent généralement pas de corrompre votre Mac, vous pourriez les faire circuler vers vos collègues utilisateurs de Windows, et ils pourraient vous affecter si vous utilisez Windows sur votre ordinateur Apple, via un programme comme Apple Boot Camp, VMware Fusion ou Parallels Desktop.
- **Analyser les e-mails :** VirusBarrier X5 analyse les courriers électroniques entrants et sortants, pour leur contenu et les pièces jointes éventuelles.
- **Analyser les iPhone / iPod touch** indique à VirusBarrier X5 d'analyser tout iPhone ou iPod touch qui est connecté à votre Mac quand vous lancez une analyse. Si cette option est décochée, VirusBarrier X5 ne montre pas un iPhone ou iPod touch dans son navigateur ou dans son étagère.
- **Analyser les archives :** Des archives contiennent un ou plusieurs fichiers, généralement en format compressé pour faciliter leur transfert. En cochant cette case, VirusBarrier X5 fait des recherches dans plusieurs formats courants d'archive, analysant non seulement le fichier d'archive lui-même, mais également les fichiers non compressés qu'il renferme. Par défaut, VirusBarrier X5 analyse tous les types d'archive qu'il peut comprendre ; cependant, vous pouvez choisir d'analyser seulement certains types d'archive en cliquant sur le bouton **Types de fichiers...**. Une fenêtre apparaît où vous pouvez sélectionner ou désélectionner les types d'archives selon vos préférences.


Analyser tous les types d'archives gérés par VirusBarrier X5
Scanner uniquement ces archives :
Apple Single
BZip
GZip
HQX
MacBinary
Pax
PaxGZ
Tar
TarBZ
TarGZ
TarZ
Unix Compress
Uuencoding
Tout sélectionner
Tout désélectionner
Annuler
OK

Préférences de planification et d'événements

Le panneau des préférences de planification et d'événements est divisé en trois sections : Affichage, Événements et Planifications.



La section Affichage contient une seule case : **Afficher les tâches planifiées dans le Gestionnaire de Tâches**. Quand la case est cochée, une petite fenêtre apparaît chaque fois que votre Mac exécute des analyses planifiées ; quand elle n'est pas cochée, de telles analyses se déroulent sans aucune notification (sauf en cas de découverte de virus).

La section Evénements permet de régler VirusBarrier X5 pour qu'il exécute automatiquement une analyse, qu'il répare ou qu'il ne fasse rien quand certains événements se produisent.

Le premier événement, **Lorsque des volumes sont montés,** est déclenché chaque fois que vous connectez un nouveau dispositif de stockage, qu'il soit local (un disque dur, par exemple) ou à distance (comme un disque réseau). Si la case **Sauf sur les volumes en lecture seule** est cochée, VirusBarrier X5 va réaliser l'action uniquement sur les volumes où il pourrait modifier le disque qui est analysé (par exemple, pour réparer un disque contenant un virus).

Le second événement, **Après la mise à jour des définitions de virus**, permet d'indiquer à VirusBarrier X5 le type d'action suite au téléchargement et à l'installation de nouvelles définitions de virus par NetUpdate. Les définitions de virus sont mises à jour régulièrement, et

particulièrement quand un nouveau virus est découvert, pour une protection adéquate. Nous vous conseillons donc de réaliser une nouvelle analyse à ces moments-là pour rechercher un nouveau virus éventuel, que ce soit manuellement ou automatiquement (en cochant cette case).

La section **Planifications** permet de déterminer quand VirusBarrier X5 va exécuter des analyses automatisées. Pour des détails sur le réglage des planifications, consultez la section Analyse planifiée au chapitre 4, **Analyse de votre Mac avec VirusBarrier X5**.

Préférences d'historique



Le panneau des préférences d'historique contient deux sections, l'une contrôlant le comportement de la fenêtre d'historique elle-même, l'autre traitant des modalités d'export des historiques d'analyse.

La section **Fenêtre d'historique** contient deux menus déroulants, pour préciser comment la fenêtre doit s'ouvrir lors des analyses et se fermer après les analyses. Chaque menu déroulant propose trois options : Jamais, Toujours et Lorsqu'un virus est trouvé / Lorsque aucun virus n'a été trouvé. Par défaut, la fenêtre d'historique reste fermée pendant les analyses, mais vous pouvez (par exemple) la régler pour qu'elle s'ouvre à chaque analyse, et pour qu'elle reste ouverte quand c'est terminé seulement si VirusBarrier X5 découvre un virus.

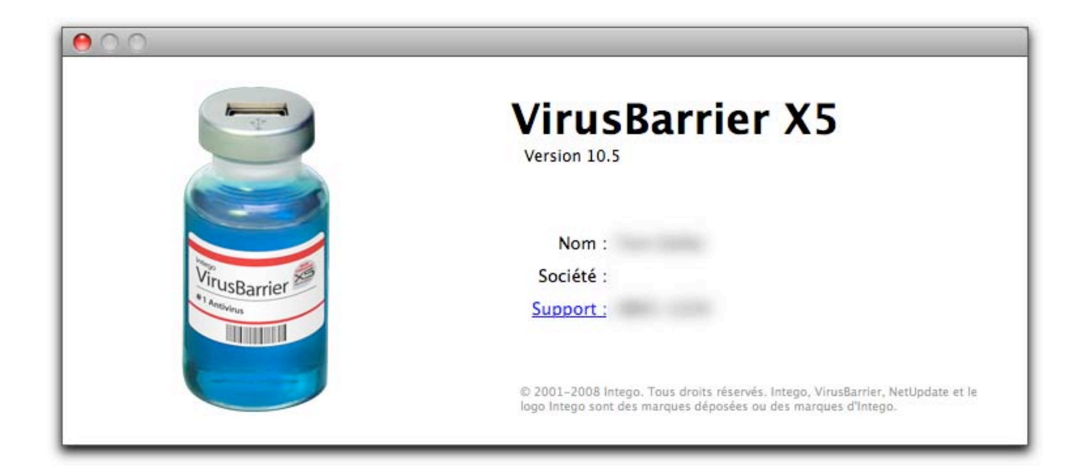
La section **Export d'historique** comprend trois menus déroulants :

- Le menu **Exporter automatiquement** propose quatre fréquences : Jamais, Chaque jour, Chaque semaine, et Chaque mois.
- Le menu **Format de fichier** propose trois options : **Texte** crée un fichier d'historique sans aucun style ni code de formatage ; **HTML** crée un fichier en texte sous style, qui est facilement lisible dans un navigateur web ; **XML** crée un fichier de données dans un format conçu pour une intégration facile avec d'autres applications reposant sur le format XML.
- Par défaut, le menu **Destination** place tous les fichiers d'historique dans le dossier /Bibliothèque/Logs/VirusBarrier. Pour modifier cet emplacement, cliquez sur **Autre...**, naviguez jusqu'au dossier voulu et cliquez sur Choisir.

Verrouillage et déverrouillage des préférences

VirusBarrier X5 propose un mode de verrouillage des préférences du programme, afin que même les utilisateurs ayant l'accès physique à votre Mac ne puissent pas modifier ses réglages. Pour verrouiller les préférences de VirusBarrier X5, soit appuyez sur Commande-L, soit choisissez Fichier > Verrouiller l'Interface. Pour déverrouiller les préférences, appuyez sur Commande-L ou choisissez Fichier > Déverrouiller l'Interface, puis entrez votre mot de passe administrateur pour terminer le processus.

À propos d'Intego VirusBarrier X5



Pour obtenir des informations sur votre copie de VirusBarrier X5, choisissez VirusBarrier X5 > À propos de VirusBarrier X5. Ce panneau donne des informations pratiques concernant VirusBarrier, comme le numéro de version, votre numéro de support (dont vous avez besoin pour le support technique), et un lien actif pour l'envoi d'un message au support technique d'Intego.

7 - Support technique

Menu Aide

L’intégralité du manuel utilisateur de VirusBarrier X5 est disponible via le menu Aide du programme. Prenez le temps de chercher une réponse à vos problèmes dans le manuel, avant de contacter le support technique d’Intego.

Support technique

Le support technique est accessible aux utilisateurs de VirusBarrier X5 qui sont enregistrés. N’oubliez pas de préciser le numéro de « build », que vous pouvez afficher en cliquant sur le numéro de version, juste au-dessus de l’icône du programme, dans la fenêtre A propos de VirusBarrier X5. Pour afficher cette fenêtre, ouvrez VirusBarrier X5 et choisissez A propos de VirusBarrier X5 dans le menu du programme.

Par courrier électronique

support@intego.com : Amérique du Nord et du Sud

eurosupport@intego.com : Europe, Moyen-Orient, Afrique

supportfr@intego.com : France

supportjp@intego.com : Japon

Sur le site web d'Intego

www.intego.com

Pour envoyer des fichiers au Centre de recherche de virus d’Intego, contactez sample@virusbarrier.com.

Vous pouvez également les mettre en surbrillance dans le Finder, maintenir la touche Ctrl enfoncée pour afficher le menu contextuel. Choisissez Plus, puis VirusBarrier X5, puis Envoyer un fichier douteux à Intego. Cela vous permet d’envoyer des fichiers, des dossiers ou des applications à Intego, sans même ouvrir votre logiciel de messagerie.

8 - Glossaire

Glossaire

Antivirus	Programme qui protège votre ordinateur contre les virus en analysant, désinfectant et réparant les fichiers infectés. Il recherche des séquences de code correspondant à la "signature" du virus dans certains emplacements dans les fichiers et les applications.
Archive	Fichier contenant plusieurs fichiers, habituellement compressé pour économiser de l'espace disque.
Boot	Démarrer un ordinateur. Le verbe vient du mot "bootstrap", au sens propre, un tirant de botte, et au sens figuré, un programme amorce, autonome.
Cheval de Troie	Un cheval de Troie, ou Troyen, est un programme derrière lequel se cache un code parasite. Étant donné qu'il ne se reproduit pas, il ne s'agit pas réellement d'un virus. Toutefois, il peut contenir un virus qui se copiera dans d'autres fichiers au moment de l'exécution du cheval de Troie. Le cheval de Troie fait référence à une tactique utilisée lors de la guerre entre Grecs et Troyens, dans l'Antiquité.
Code	Les programmes informatiques sont écrits sous forme de code (ou langage de programmation). Étant des programmes informatiques, les virus sont également écrits sous forme de code.
Commande macro	Commande de programmation qui peut être exécutée dans une macro. Elle exploite le langage macro propre à l'application utilisée.
Infecter	On dit qu'un fichier est infecté lorsqu'un virus s'est copié dans ce fichier. Il peut s'agir d'une macro copiée dans un fichier de traitement de texte, ou d'un autre type de code copié dans une application.
Macro	Petit programme utilisant les fonctions intégrées du langage macro d'une application. De nombreuses applications offrent des fonctions macro afin de faciliter l'exécution des tâches répétitives. Hélas, les macros peuvent contenir des virus et les virus macro en circulation sont très nombreux, notamment ceux qui s'exécutent sous Microsoft Word ou Excel.
Partition	Une partition (ou volume) est une division logique de disque dur. Il est possible d'en créer plusieurs sur un disque dur. Chacune fonctionne alors comme un petit disque dur. Le système d'exploitation considère les partitions comme des volumes distincts.
Souche	Variation ou mutation d'un certain virus. Tout comme il est employé en

	médecine pour désigner les mutations de virus biologiques, ce terme s'applique aux virus informatiques qui, dans certains cas, subissent une mutation et donnent naissance à de nouvelles souches.
Support amovible	Tout support de stockage de données s'insérant dans un lecteur, tel que CD ou DVD.
Ver	Un ver est un programme qui se propage sur un réseau en s'auto-reproduisant. Du fait de leur capacité à nuire, on considère souvent les vers comme une variété de virus. Ils ne fonctionnent cependant pas de la même manière. Les vers n'ont pas besoin de fichiers hôtes pour se reproduire.
Virus	Programme informatique ou séquence de code informatique capable de se reproduire et de se propager. La plupart des virus sont malveillants et infectent les fichiers en s'attachant à eux. Ils se propagent ensuite à l'ouverture ou à l'exécution des fichiers hôtes.
Virus macro	Virus exploitant le langage macro intégré d'une application. Les virus macro sont actuellement les virus les plus redoutables pour les utilisateurs de Macintosh, particulièrement ceux qui s'exécutent sous Microsoft Word ou Excel, puisqu'ils sont transmissibles entre ordinateurs Macintosh et ordinateurs sous Windows.
Volume	Un volume est, par essence, un disque dur ou un support amovible. Il peut s'agir d'un disque dur entier, d'une partition de disque dur, d'un ordinateur de réseau distant ou d'une disquette. Sa spécificité est de contenir ses propres fichiers répertoires indiquant où sont stockés les fichiers.